中国光学（中英文） Chinese Optics 核心期刊

大气多输入-多输出光信道共享密钥提取研究

陈纯毅 蔡锦湘 李琼

Shared secret-key extraction from atmospheric MIMO optical channel

CHEN Chun-yi, CAI Jin-xiang, LI Qiong

引用本文:
陈纯毅, 蔡锦湘, 李琼. 大气多输入-多输出光信道共享密钥提取研究[J]. 中国光学, 2024, 17(5): 1219-1226. doi: 10.37188/CO.2023-0202
CHEN Chun-yi, CAI Jin-xiang, LI Qiong. Shared secret-key extraction from atmospheric MIMO optical channel[J]. *Chinese Optics*, 2024, 17(5): 1219-1226. doi: 10.37188/CO.2023-0202

在线阅读 View online: https://doi.org/10.37188/CO.2023-0202

您可能感兴趣的其他文章

Articles you may be interested in

扭曲拉盖尔—高斯关联光束对大气湍流传输影响的抑制
Suppression of the influence of atmospheric turbulence during the propagation of a twisted Laguerre-Gaussian correlated beam
中国光学（中英文）. 2021, 14(3): 704 https://doi.org/10.37188/CO.2020-0138

大气湍流对高分辨率遥感卫星定位精度的影响分析
Effect of atmospheric turbulence on the tracking accuracy of high-resolution remote sensing satellites
中国光学（中英文）. 2023, 16(3): 550 https://doi.org/10.37188/CO.2022-0196

斜程湍流大气中部分相干艾里光束的偏振特性研究
Polarization changes of partially-coherent Airy-Gaussian beams in a slanted turbulent atmosphere
中国光学（中英文）. 2021, 14(2): 409 https://doi.org/10.37188/CO.2020-0095

基于互补集合经验模态分解结合希尔伯特变换的光频扫描干涉信号相位提取方法
Phase-extracting method of optical frequency scanning interference signals based on the CEEMD-HT algorithm
中国光学（中英文）. 2023, 16(3): 682 https://doi.org/10.37188/CO.2022-0173

超光谱分辨率紫外双通道共光路成像光谱仪设计
Hyperspectral resolution ultraviolet dual channel common optical path imaging spectrometer
中国光学（中英文）. 2022, 15(5): 1029 https://doi.org/10.37188/CO.2022-0125

基于大气多次散射的波浪水下偏振模式研究
The polarization mode of underwater waves based on atmospheric multiple scattering
中国光学（中英文）. 2023, 16(6): 1324 https://doi.org/10.37188/CO.2022-0223

文章编号　2097-1842(2024)05-1219-08

大气多输入-多输出光信道共享密钥提取研究

陈纯毅[1,2,3]*, 蔡锦湘[1,3], 李　琼[1,3]
（1. 长春理工大学 空地激光通信技术国防重点学科实验室, 吉林 长春 130022;
2. 长春理工大学 重庆研究院, 重庆 401135;
3. 长春理工大学 计算机科学技术学院, 吉林 长春 130022）

摘要: 基于信道随机特征的共享密钥提取是实现大气光信道物理层安全的一种有效手段。密钥生成速率和不一致率是关注焦点。利用大气湍流光信道随机特征作为共享随机源, 提出多输入-多输出 (multiple-input multiple-output, MIMO) 大气光信道环境下的密钥提取方案。采用另类奇异值分解法来分解信道矩阵, 通过简单移动平均提升合法双方获得的信道特征序列间的相关性, 并对移动平均后的信道特征序列进行单门限交错量化。合法双方基于分集差分值生成编码映射控制随机序列, 实现对信道特征序列的单门限交错量化结果的编码映射。实验结果表明, 本文方案的原始密钥不一致率在信噪比为 30 dB 时能够达到 4.5×10^{-5}, 且生成的随机比特序列可通过美国国家标准与技术研究院 (NIST) 的随机性测试。本文结果对 MIMO 大气光信道密钥提取有一定参考价值。

关　键　词: MIMO; 光信道; 大气湍流; 密钥提取; 量化
中图分类号: TP929.12　　**文献标志码:** A　　**doi:** 10.37188/CO.2023-0202

Shared secret-key extraction from atmospheric MIMO optical channel

CHEN Chun-yi[1,2,3]*, CAI Jin-xiang[1,3], LI Qiong[1,3]
（1. *Key Laboratory for Defense Discipline of Space-to-Ground Laser Communication Technology*, *Changchun* 130022, *China*;
2. *Chongqing Research Institute*, *Changchun University of Science and Technology*, *Chongqing* 401135, *China*;
3. *School of Computer Science and Technology*, *Changchun University of Science and Technology*, *Changchun* 130022, *China*）
* *Corresponding author*, *E-mail*: *chenchunyi@hotmail.com*

Abstract: Shared secret-key extraction from random channel characteristics is an effective approach to ensuring the physical layer security of atmospheric optical channels. The secret-key generation rate and disagreement rate are two issues that attract a lot of attention. Using the random characteristics of atmospheric turbulent optical channels as a shared source of randomness, a secret-key extraction scheme for multiple-input multiple-output (MIMO) atmospheric optical channels is proposed. The alternative singular value decomposition is used to decompose the channel matrix; the correlation between the two channel characteristic se-

收稿日期: 2023-11-10; **修订日期:** 2023-12-13
基金项目: 国家自然科学基金资助项目(No. 62275033); 重庆市自然科学基金项目(No. cstc2021jcyj-msxmX0457)
Supported by the National Natural Science Foundation of China (No. 62275033); the Natural Science Foundation of Chongqing City of China (No. cstc2021jcyj-msxmX0457)

quences obtained by the two legitimate parties is enhanced through a simple moving average, and the single-threshold interleaved quantization is performed on the channel characteristic sequences after moving average. The two legitimate parties generate random controlling sequences for coding mapping based on differential diversity values, in order to implement encoding mapping for the single threshold interleaved quantization results of the channel characteristic sequences. The experimental results show that our scheme's initial key disagreement rate can reach 4.5×10^{-5} at a signal-to-noise ratio of 30 dB, and that the generated random bit sequences have passed the National Institute of Standards and Technology (NIST) randomness test. The results are useful in the implementation of secret-key extraction from atmospheric MIMO optical channels.

Key words: MIMO; optical channel; atmospheric turbulence; secret-key extraction; quantization

1 引 言

当前信息传输安全受到广泛关注。以往通常使用对称加密的方式以保护传输的信息，避免其被非法窃取，这种方式需先使用公钥机制为收发双方分配共享密钥，然后再利用共享密钥通过对称加密体制来保护信息。然而，公钥机制无法确保信息论安全。量子密钥分发[1]是一种能实现信息论安全的共享密钥分配技术，但是量子密钥分发需要使用量子器件，成本相对较高。最近几年，研究人员将目光聚焦在基于无线信道随机特征的共享密钥提取上。国内外研究者对不同信道的共享密钥提取均开展了一系列研究，例如基于大气光信道[2-4]和无线电信道[5-8]的共享密钥提取。后者多数针对室内环境，例如室内 wifi[5]、蓝牙[6]通信等，在无线电信道中可利用不同的信道随机特征提取密钥，例如接收信号强度、信道冲激响应、信道频率响应等[7-10]。从大气光信道中提取密钥很适合大气环境中远距离共享密钥生成的应用场景。理论和实验[2-4]都已经证明，在使用收发共模耦合方式时，大气湍流光信道能够保持良好的互易性。大气湍流扰动使光信道特征发生随机变化，从其中可以提取随机密钥[9-11]。

在同一个信道自相关时间内的多次信道测量值具有很强的相关性。为了确保生成密钥的随机性，要求信道测量时间间隔大于信道自相关时间，而密钥生成速率受到信道自相关时间长度的限制。传统上主要从信道的时域随机性中提取密钥，然而，实际上也可以利用信道的空域随机性来进一步提高密钥生成速率。鉴于此，文献 [3] 指出可以利用多输入-多输出 (MIMO) 大气光信道来提高密钥生成速率。本文考虑在 MIMO 大气光信道环境下进行密钥提取，提出一种基于奇异值分解的信道特征量化方案。对信道矩阵进行另类奇异值分解（alternative singular value decomposition, ASVD）[11]。根据分解后的矩阵得到信道特征序列，对信道特征序列采用简单移动平均处理，合法双方对处理后的序列进行单门限交错量化[12]。根据分集差分值用阈值量化得到编码映射控制序列，使用此序列对单门限交错量化后的比特进行随机编码映射。该方案利用分集差分值的随机性，可增加单位时间内密钥比特数。

2 系统模型

本文所考虑的光信道是一个双向空间分集光信道，如图 1 所示。合法双方（Alice 和 Bob）分别位于信道的两端，此外，本文考虑一个被动窃听者 Eve。在窃听过程中，Eve 很难在截获光束主瓣的条件下不被合法双方察觉。因此 Eve 只能在靠近 Alice 或 Bob 的光束发散区域内窃听，接收在合法方接收孔径范围外的光信号。假设 Alice 有 N_A 个光信号收发器，Bob 有 N_B 个光信号收发器，Eve 有 N_E 个光信号接收器。合法双方既可以向对方发送光信号也可以接收对方发来的光信号，光信号穿过的空间中存在大气湍流，使得光信号在传播过程中会产生随机衰落。

在信道探测过程中，合法双方按照图 2 所示的方式向对方发送光信号。t_0至t_2时段为一个时间帧，一个时间帧包含多个时隙，一个时隙的时间长度为τ_s，一个时间帧的时间长度为τ_c，完整的信道探测一共包括 N_p 个时间帧。$a_{i,k}$表示 Alice 的

第 i 个发送器在第 k 个时间帧向对方发送光信号的时隙, i=1, 2, ⋯, N_A, k=1, 2, ⋯, N_p。$b_{j,k}$表示 Bob 的第 j 个发送器在第 k 个时间帧向对方发送光信号的时隙 j=1, 2, ⋯, N_B。为保证合法双方在同一个时间帧内测量到相关性较高的信道特征, τ_c要小于或等于信道自相关时间。为保证不同时间帧测量到的信道特征具有低相关性, 时间帧的间隔τ_p(从 t_2 到 t_3 的时段)应大于信道自相关时间。

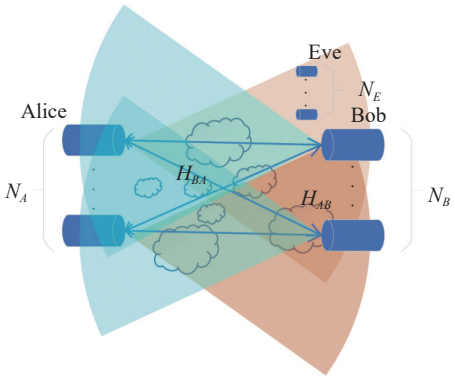

图 1　大气 MIMO 光信道示意图

Fig. 1　Schematic diagram of atmospheric MIMO optical channel

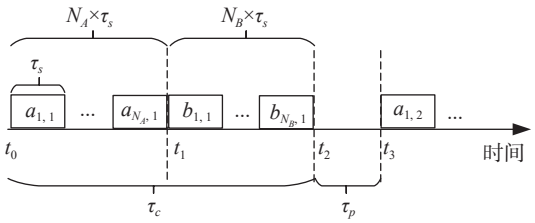

图 2　合法双方信号发送帧结构

Fig. 2　Frame structure for signal transmission between legitimate parties

在第 k 个时间帧中, Alice 的第 i 个光信号接收器探测到来自 Bob 的第 j 个光信号发送器发送的信号:

$$y_{A,k,i,j} = RP_t\alpha_{i,j}h_{BA,k,j,i}S + n_{A,k,i,j} \quad , \qquad (1)$$

式中, R 为探测器响应度, P_t为发射功率, $\alpha_{i,j}$为不存在大气湍流时的功率衰减系数, $h_{BA,k,j,i}$ 表示在第 k 帧时从 Bob 的第 j 个光发送器到 Alice 的第 i 个光接收器的瞬时信道衰落系数, $S\equiv 1$ 为发送的训练信号, $n_{A,k,i,j}$ 表示白高斯探测噪声。

在第 k 个时间帧中, Bob 的第 j 个光接收器探测到来自 Alice 的第 i 个光发送器发送的信号, 为:

$$y_{B,k,j,i} = RP_t\alpha_{j,i}h_{AB,k,i,j}S + n_{B,k,j,i} \quad , \qquad (2)$$

式中, $\alpha_{j,i}$为不存在大气湍流时的功率衰减系数, $h_{AB,k,i,j}$ 表示在第 k 帧时从 Alice 的第 i 个光发送器到 Bob 的第 j 个光接收器的瞬时信道衰落系数, $n_{B,k,j,i}$ 表示白高斯探测噪声。后面将用下标“A”标识合法用户 Alice, “B”标识合法用户 Bob。由于 τ_c小于信道自相关时间, 故同一时间帧内信道具有互易性, 有 $h_{BA,k,j,i}$=$h_{AB,k,i,j}$。双方在第 k 个时间帧分别测量到的信道矩阵$\boldsymbol{H}_{AB,k}$和$\boldsymbol{H}_{BA,k}$的各元素估计值分别为:

$$\widetilde{h}_{AB,k,i,j} = h_{AB,k,i,j} + \tilde{n}_{B,k,j,i}, \qquad (3)$$

$$\widetilde{h}_{BA,k,j,i} = h_{BA,k,j,i} + \tilde{n}_{A,k,i,j}, \qquad (4)$$

其中, $\widetilde{h}_{AB,k,i,j}$表示信道矩阵$\boldsymbol{H}_{AB,k}$的第 i 行、第 j 列元素, $\widetilde{h}_{BA,k,j,i}$表示信道矩阵$\boldsymbol{H}_{BA,k}$的第 j 行、第 i 列元素, $\widetilde{n}_{A,k,i,j} = n_{A,k,i,j}/(RP_t\alpha_{i,j})$, $\widetilde{n}_{B,k,j,i} = n_{B,k,j,i}/(RP_t\alpha_{j,i})$, $\boldsymbol{H}_{AB,k}\in\mathbb{R}^{N_A\times N_B}$、$\boldsymbol{H}_{BA,k}\in\mathbb{R}^{N_B\times N_A}$, 当不存在探测噪声影响时有$\boldsymbol{H}_{AB,k} = \boldsymbol{H}_{BA,k}^{\mathrm{T}}$。

3　基于随机编码映射的密钥提取

3.1　总体流程

本文总体流程如图 3 所示。首先, 合法双方在完成信道探测后, 得到带有加性高斯噪声的信道矩阵。接着, 对信道矩阵执行 ASVD, 合法双方对执行 ASVD 后得到的矩阵进行横向拼接, 获得 N_A 个行向量, 对每个行向量进行简单移动平均处理, 得到行向量的集合$\{\boldsymbol{r}_{u,i}^{(1)}\}$, 其中 u 为“A”或“B”, $\boldsymbol{r}_{u,i}^{(1)}$为集合中的第 i 个行向量, $i\in\{1, 2, \cdots, N_A\}$。接下来, Alice 指定编码映射表长度 Q_l 并通知 Bob。合法双方生成包含 Q_l 个条目的编码映射表 $\boldsymbol{M}$, 并对$\{\boldsymbol{r}_{u,i}^{(1)}\}$中的不同行向量元素的差分值进行阈值量化。拼接后得到 $\boldsymbol{d}_u$。对$\{\boldsymbol{r}_{u,i}^{(1)}\}$的行向量进行拼接得到$\hat{\boldsymbol{r}}_u^{(1)}$, 再对$\hat{\boldsymbol{r}}_u^{(1)}$进行单门限交错量化[12]得到二进制序列$\boldsymbol{r}_u^{(2)}$。把 $\boldsymbol{d}_u$ 的每 $\log_2 Q_l$ 位比特表示的二进制值当作一个索引值, 得到编码映射控制序列$\boldsymbol{r}_u^{(3)}$。最后, 根据编码映射表 $\boldsymbol{M}$ 和$\boldsymbol{r}_u^{(3)}$完成对$\boldsymbol{r}_u^{(2)}$的随机编码映射, 生成原始密钥。交错量化可以视为基于量化指示位的自适应边界

偏移量化算法，Bob 需要根据 Alice 传来的量化指示位调整自己的量化边界。在本方案的整个量化过程中，合法双方传送的数据内容不会泄露密钥信息，Eve 无法通过窃听获得和合法双方相同的密钥。接下来将对本方案的各步骤进行详细说明。

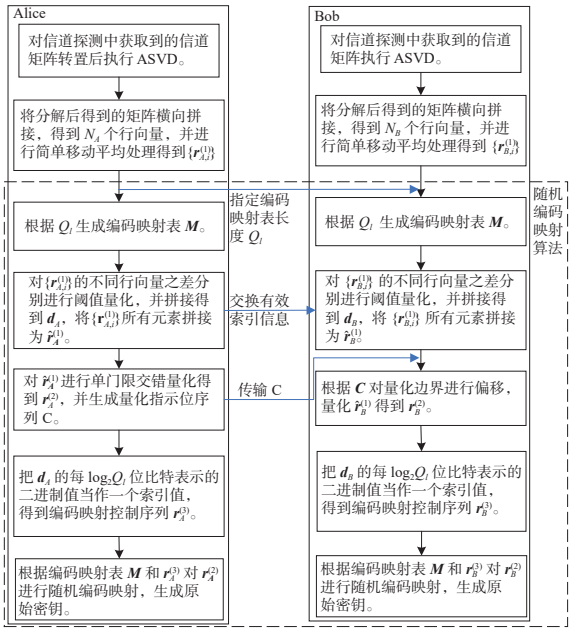

图 3　密钥提取总体流程

Fig. 3　Flow chart of secret-key extraction

3.2　另类奇异值分解

文献 [11] 提出了两种基于奇异值分解的量化方案：第一种是 Alice 和 Bob 对信道矩阵进行奇异值分解后，对得到的左、右奇异值矩阵进行量化；第二种是先对信道矩阵进行 ASVD，再对分解得到的矩阵进行量化。假设 $m\geqslant n$，ASVD 可以将一个 $m\times n$ 的秩为 n 的矩阵分解为 n 个 $m\times n$ 的带权矩阵和。本文采用第二种分解方式对信道矩阵进行处理。合法双方按下面的方式对信道矩阵进行分解，首先进行奇异值分解：

$$\boldsymbol{H}_u^* = \boldsymbol{U}\boldsymbol{D}\boldsymbol{V}^{\mathrm{T}} \quad , \tag{5}$$

其中 u 为“A”或“B”，$\boldsymbol{H}_A^* = \boldsymbol{H}_{BA,k}^{\mathrm{T}}$，$\boldsymbol{H}_B^*=\boldsymbol{H}_{AB,k}$，$\boldsymbol{H}_u^* \in \mathbb{R}^{N_A\times N_B}$。设$N_A\geqslant N_B$，信道矩阵秩为$N_B$，$\boldsymbol{U}\in\mathbb{R}^{N_A\times N_A}$，$\boldsymbol{V}\in\mathbb{R}^{N_B\times N_B}$，$\boldsymbol{H}_u^*$可以继续被分解为$N_B$个矩阵的加权和[11]，分解方式为：

$$\boldsymbol{H}_u^* = \sum_{i=1}^{N_B}\boldsymbol{A}_i = \sum_{i=1}^{N_B}\sigma_i\boldsymbol{u}_i\boldsymbol{v}_i^{\mathrm{T}} \quad , \tag{6}$$

式中，$\boldsymbol{A}_i$为分解后的第i个矩阵，$\boldsymbol{A}_i\in\mathbb{R}^{N_A\times N_B}$，$\boldsymbol{u}_i$、$\boldsymbol{v}_i$分别为$\boldsymbol{U}$、$\boldsymbol{V}$的第$i$个列向量，$\sigma_i$为第$i$个奇异值，$i\in\{1,2,\cdots,N_B\}$。ASVD 将大小为$N_A\times N_B$的信道矩阵分解得到$N_B$个$N_A\times N_B$的矩阵。通过对$\boldsymbol{A}_i$进行后续量化操作，可提升密钥生成率。文献 [11] 对于量化后的原始密钥仅进行了游程检测，未进行完整的美国国家标准与技术研究院（NIST）随机性测试，故不能完全保证其随机性。本方案通过加入随机编码映射，保证量化得到的密钥序列能够通过完整的 NIST 随机性测试，另外还可以增加密钥长度。

3.3　简单移动平均

Zhan 等人[13] 通过实验说明，双向信道两个方向的主要信道变化是相似的，但由于存在硬件噪声等干扰，导致信道两端的信道测量值出现不同的小尺度波动。可以将此波动理解为信道的次要变化，这是由信道测量噪声引起的。这样的噪声在量化阶段会使双方相同索引位的信道特征值被分到不同的编码区间，造成量化得到的原始密钥序列出现不一致比特。合法双方原始密钥差异过大会导致量化之后的信息协商效率低、不安全且占用大量的计算资源和通信带宽。因此有必要对信道特征序列进行一些处理来削弱噪声的影响。在众多降噪算法中，简单移动平均 (simple moving average, SMA)[13] 效果明显且时间复杂度低，因此本方案采用 SMA 对信道特征序列进行处理。合法双方将 ASVD 生成的矩阵$\{\boldsymbol{A}_i\}$进行横向拼接（即把 N_p 个信道矩阵分解得到的 $\boldsymbol{A}_1$ 至 $\boldsymbol{A}_{N_B}$ 的具有相同行号的行拼接在一起），得到N_A个行向量，行向量长度为 $l_1=N_p\times N_B^2$，对每个行向量进行 SMA 处理得到行向量集合$\{\boldsymbol{r}_{u,i}^{(1)}\}$，$i\in\{1,2,\cdots,N_A\}$，其中第 i 个行向量的第 n 个元素的值为：

$$\tilde{r}_{u,i}^{(1)}(n) = \frac{1}{w}\sum_{m=n-\lfloor w/2\rfloor}^{n+\lfloor w/2\rfloor} r_{u,i}^{(1)}(m) \quad , \tag{7}$$

式中 u 为“A”或“B”，w 为窗口大小，$r_{u,i}^{(1)}(m)$为 SMA 处理前的第 i 个行向量的第 m 个元素，$\lfloor x\rfloor$表示对 x 向下取值：当 $m>l_1$ 时，m 对 l_1 取余；当 $m<l_1$ 时，$m=l_1+m$。$\boldsymbol{r}_{A,i}^{(1)}$与$\boldsymbol{r}_{B,i}^{(1)}$的皮尔逊相关系数随移动平均窗口尺寸的变化情况如图 4 所示。窗口越大噪声影响越小，由图 4 可知，随着窗口 w 的增大，$\boldsymbol{r}_{A,i}^{(1)}$与$\boldsymbol{r}_{B,i}^{(1)}$间的相关性系数随之升高。

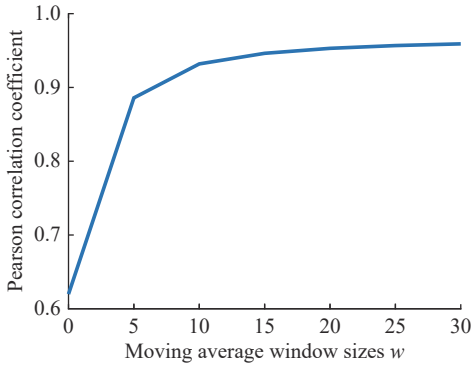

图 4　不同移动平均窗口下$\boldsymbol{r}_{A,i}^{(1)}$与$\boldsymbol{r}_{B,i}^{(1)}$的皮尔逊相关系数

Fig. 4　Pearson correlation coefficient between $\boldsymbol{r}_{A,i}^{(1)}$ and $\boldsymbol{r}_{B,i}^{(1)}$ at different moving average window sizes

Yang 等人[14] 的实验结果表明, 上述处理方式需要在消除噪声和保持密钥随机性之间找到平衡。对于 SMA 的处理, 当窗口增大时, 消除噪声的效果会更明显, 但同时也会消除部分由大气湍流引起的随机变化。因此, 当窗口大小超过某个阈值时, 向量元素的自相关性会提升, 从而影响提取密钥的随机性。考虑到这一点, 本方案将采用随机编码映射以提供更多随机性。

3.4　基于分集差分值生成编码映射控制序列

通过分集差分值的阈值量化得到二进制随机序列$\boldsymbol{d}_u$, 再基于$\boldsymbol{d}_u$和 Q_l 生成编码映射控制随机序列$\boldsymbol{r}_u^{(3)}$, 其中 u 为“A”或“B”。$\boldsymbol{r}_u^{(3)}$在随机编码映射算法中充当控制映射的角色。本文基于分集差分值生成$\boldsymbol{r}_u^{(3)}$, 从而可利用空域随机熵为最终的密钥提供更多随机性。本文研究的是 MIMO 环境, 可以利用信道的快速空间退相关性进行处理。通过信道矩阵经过 ASVD 后的不同行向量$\boldsymbol{r}_{u,i}^{(1)}$之差获取差分值。具体过程如下: 对于合法用户 u, 基于分集差分值得到二进制序列$\boldsymbol{d}_u$。合法双方对集合$\{\boldsymbol{r}_{u,i}^{(1)}\}$的第 i 个行向量与第 i+1 个行向量的第 m 个元素的差分值及第N_A个行向量与第1个行向量第 m 个元素的差分值进行阈值量化。使用的双阈值量化函数如下:

$$F_Q(\tilde{r}_{u,i}^{(1)}(m),\tilde{r}_{u,i+1}^{(1)}(m))=\begin{cases}1, & \tilde{r}_{u,i+1}^{(1)}(m)-\tilde{r}_{u,i}^{(1)}(m)>\varepsilon_{u,+}\\ 0, & \tilde{r}_{u,i+1}^{(1)}(m)-\tilde{r}_{u,i}^{(1)}(m)<\varepsilon_{u,-}\\ \text{无效}, & \varepsilon_{u,-}\leqslant\tilde{r}_{u,i+1}^{(1)}(m)-\tilde{r}_{u,i}^{(1)}(m)\leqslant\varepsilon_{u,+}\end{cases},\tag{8}$$

式中, $\varepsilon_{u,-}$和$\varepsilon_{u,+}$是两个阈值。合法双方输入集合$\{\boldsymbol{r}_{u,i}^{(1)}\}$中的行向量元素进行差分值阈值量化, 以得到随机序列$\boldsymbol{d}_u$。完成这一步后合法双方将$\{\boldsymbol{r}_{u,i}^{(1)}\}$中所有元素进行拼接得到行向量$\hat{\boldsymbol{r}}_u^{(1)}$。$\hat{\boldsymbol{r}}_u^{(1)}$的长度 $l_2=l_1\times N_A$。

Alice 和 Bob 使用双阈值量化来降低$\boldsymbol{d}_A$和$\boldsymbol{d}_B$的不一致率, 其中样本丢弃率 r 依赖于选定的两个阈值$\varepsilon_{u,-}$和$\varepsilon_{u,+}$。将 Alice 和 Bob 一方无效或双方都无效的比特位删除, 得到随机比特序列$\boldsymbol{d}_u$。$\boldsymbol{d}_u$长度为 l_d。由于双方的有效比特位不完全重合且只保留双方都有效的比特位, 所以最终丢弃率会略大于 r。

3.5　随机编码映射算法

对于密钥提取量化, 在算法相同的情况下, 量化区间越多, 密钥生成率越高, 同时密钥不一致率也越高。合法双方先对$\hat{\boldsymbol{r}}_u^{(1)}$进行单门限交错量化[12] 得到随机的二进制序列$\boldsymbol{r}_u^{(2)}$, 保证较低的密钥不一致率, 再通过随机编码映射扩展密钥长度。本文的单门限交错量化区间个数 Q_R=2, 具体量化过程为: Alice 确定能将自己的样本等概率地分成两个部分的量化区间边界, 并据此对样本进行单阈值量化; Alice 把每个量化区间分成两个等概率的子区间, 在样本量化过程中, 记录样本落入量化区间的哪个子区间, 据此生成指示位; Alice 把指示位传给 Bob; 与 Alice 类似, Bob 确定能把自己的样本等概率地分成两个部分的量化区间边界; 对每个样本, Bob 根据 Alice 发来的指示位自适应地移动量化区间边界, 以减小 Alice 和 Bob 量化生成的密钥比特不一致率。由于 Alice 和 Bob 的量化区间因量化区间边界平移而出现交错, 故称为交错量化。

$\hat{\boldsymbol{r}}_u^{(1)}$为 $1\times l_2$ 的行向量, 经过单门限交错量化后得到的$\boldsymbol{r}_u^{(2)}$是长为 l_2 的随机序列。合法双方根据$\boldsymbol{d}_u$和 Q_l 生成编码映射控制随机序列$\boldsymbol{r}_u^{(3)}$, $\boldsymbol{r}_u^{(3)}$长度为$l_3=\lfloor l_d/\log_2 Q_l\rfloor$。生成规则是把 $\boldsymbol{d}_u$ 分割成一系列包含 $\log_2 Q_l$ 位的比特子串。每个子串对应的二进制值为一个索引值, 从而得到$\boldsymbol{r}_u^{(3)}$。$\boldsymbol{r}_u^{(3)}$的第 m 个元素$r_u^{(3)}(m)\in\{0,1,\cdots,Q_l-1\}$, u 为“A”或“B”, $m\in\{1,2,\cdots,l_3\}$。

随机编码映射过程如图 5 所示, 根据$\log_2 Q_l$

位的格雷码表生成 Q_l 行、2 列的编码映射表 $\boldsymbol{M}$。$\boldsymbol{M}$ 的第一列第 j 行是格雷码表的第 j 行编码，$\boldsymbol{M}$ 的第二列第 j 行是格雷码表的第 $(j+1)\%Q_l$ 行编码，$x\%y$ 表示 x 对 y 取余，$j\in\{1, 2, \cdots, Q_l\}$。使用 $r_u^{(3)}(m)$ 和 $\boldsymbol{M}$ 对 $r_u^{(2)}(n)$ 进行随机编码映射，$n\in\{1, 2, \cdots, l_2\}$，$m\in\{1, 2, \cdots, l_3\}$。

由图 5 可知，首先通过 $r_u^{(3)}(m)$ 确认行号，再通过 $r_u^{(2)}(n)$ 确认列号，编码映射表 $\boldsymbol{M}$ 中相应行、列位置的编码即为编码映射生成的密钥子串（当 m 大于 l_3 时，m 从 1 开始重新循环）。通过实施编码映射，得到原始密钥序列 $\boldsymbol{q}_u$，$u\in\{A, B\}$。$\boldsymbol{q}_u$ 长度为 $l_q=l_2\times\log_2 Q_l$。

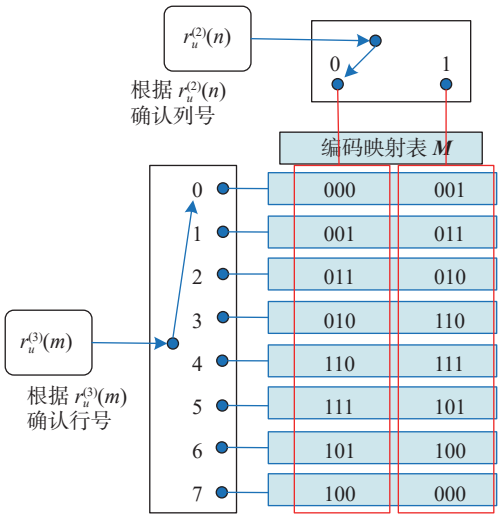

图 5 Q_l=8 时的编码映射示意图

Fig. 5 Schematic diagram of encoding mapping with Q_l =8

4 性能评估与结果比较

使用原始密钥不一致率 p_{KDR} 来评估本方案的性能，其定义式为：

$$p_{\mathrm{KDR}}=\frac{1}{l_q}\sum_{i=1}^{l_q}\mathbb{I}(q_A(i)\neq q_B(i)) \quad , \qquad (9)$$

其中 $q_u(i)$ 为原始密钥序列 $\boldsymbol{q}_u$ 的第 i 位，u=“A”或“B”，i=1, 2, ⋯, l_q；$\mathbb{I}(x)$ 为指数函数，当参数 x 为真时 $\mathbb{I}(x)=1$，反之，$\mathbb{I}(x)=0$。在基于共享信道的密钥提取中，噪声是导致双方密钥不一致的主要原因。为评估方案性能，在不同的信噪比 γ_{SNR} 下进行测试。本文测试了基于奇异值分解的信道量化 (channel quantization with singular value decomposition, CQSVD) 方案[11]、信道交错量化（channel quantization alternating, CQA）方案[12]，并用蒙特卡罗方法计算不同 γ_{SNR} 下的原始密钥不一致率，如图 6 所示。本节实验设置 N_A=4、N_B=3，Q_l=8，CQA 及 CQSVD 的量化区间数量 Q_R=8。图 6 中的横坐标表示不同大小的信噪比 γ_{SNR}。显然，在不同信噪比 γ_{SNR} 下，本文方案的原始密钥不一致率都最低。这是因为本文方案先通过单门限交错量化产生密钥，再通过随机编码映射扩展密钥，使得密钥不一致率更低。

为验证生成的原始密钥的有效性，本文使用 NIST 随机性测试套件[15] 验证原始密钥的随机性，如表 1 所示。可见，11 个测试项的 P-value 值都大于 0.01，由此可知产生的原始密钥通过了 NIST 随机性测试，说明原始密钥序列足够随机。

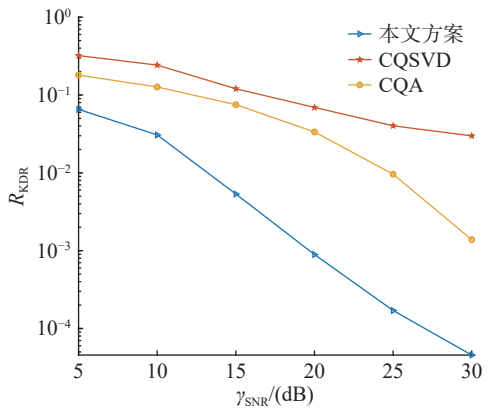

图 6 不同方案的原始密钥不一致率对比图

Fig. 6 Comparison chart of initial key disagreement rate for different schemes

表 1 NIST 随机性测试结果

Tab. 1 NIST randomness test results

Test	Average P-value
频率	0.066 882
块内频率	0.058 146
游程	0.350 485
最大游程	0.213 309
二进制矩阵秩	0.065 429
离散傅立叶变换	0.534 971
非重叠字匹配	0.739 913
重叠字匹配	0.911 413
线性复杂度	0.739 918
串行	0.122 325 0.035 174
累积和	0.064 229 0.067 324

5 结　论

本文设计了一种在大气 MIMO 光信道环境下的随机密钥提取方案。在量化过程中，合法双方需要传送的数据只有索引信息和量化指示位，从而不会泄露密钥信息，可以保证第三方无法通过窃听获得与合法双方相同的密钥。本方案的随机编码映射操作可实现在使用单门限量化的情况下，使每个送入量化器的随机特征值最终生成 $\log_2 Q_l$ 个比特（$Q_l \geqslant 2$）。由于使用了交错量化策略，本文方案显著降低了合法双方原始密钥的不一致率。与现有量化方案相比，本文方案在密钥不一致率上具有显著优势。此外，本文生成的原始密钥序列已通过 NIST 随机性测试。

本方案使用大气 MIMO 光信道提取随机密钥，可以充分利用空域随机熵，提升了密钥生成速率。本文方案在信噪比为 30 dB、Q_l=8、N_A=4、N_B=3 的情况下，原始密钥不一致率能够达到 4.5×10^{-5}。

参考文献:

[1] 王潋, 周媛媛, 周学军, 等. 泡沫覆盖不规则海面的非均匀空-水信道量子密钥分发[J]. 中国光学 (中英文), 2019, 12(6): 1362-1375.
WANG L, ZHOU Y Y, ZHOU X J, *et al*.. Quantum key distribution based on heterogeneous air-water channels with foam-covered irregular sea surfaces[J]. *Chinese Optics*, 2019, 12(6): 1362-1375. (in Chinese).

[2] 向磊, 陈纯毅, 姚海峰, 等. 双向大气湍流光信道瞬时衰落相关特性测量[J]. 中国光学 (中英文), 2019, 12(5): 1100-1108.
XIANG L, CHEN CH Y, YAO H F, *et al*.. Measurement of instantaneous-fading correlation in bidirectional optical channels through atmospheric turbulence[J]. *Chinese Optics*, 2019, 12(5): 1100-1108. (in Chinese).

[3] CHEN CH Y, YANG H M. Shared secret key generation from signal fading in a turbulent optical wireless channel using common-transverse-spatial-mode coupling[J]. *Optics Express*, 2018, 26(13): 16422-16441.

[4] CHEN CH Y. Sample-grouping-based vector quantization for secret key extraction from atmospheric optical wireless channels[J]. *IEEE Transactions on Wireless Communications*, 2022, 21(11): 8905-8918.

[5] WANG L, AN H N, ZHU H J, *et al*.. MobiKey: mobility-based secret key generation in smart home[J]. *IEEE Internet of Things Journal*, 2020, 7(8): 7590-7600.

[6] 黄开枝, 金梁, 钟州. 5G 物理层安全技术——以通信促安全[J]. 中兴通讯技术, 2019, 25(4): 43-49.
HUANG. K ZH, JIN L, ZHONG ZH. 5G physical layer security technology: enhancing security by communication[J]. *ZTE Technology Journal*, 2019, 25(4): 43-49. (in Chinese)

[7] HUANG L, GUO D K, XIONG J, *et al*. . An improved CQA quantization algorithm for physical layer secret key extraction[C]. *Proceeding of the 2020 International Conference on Wireless Communications and Signal Processing* (*WCSP*), IEEE, 2020: 829-834.

[8] TANG J, WEN H, SONG H H, *et al*.. Secure MIMO-SVD communications against eavesdroppers with any number of antennas[J]. *IEEE Transactions on Vehicular Technology*, 2020, 69(10): 11077-11089.

[9] PREMNATH S N, GOWDA P L, KASERA S K, *et al*. . Secret key extraction using Bluetooth wireless signal strength measurements[C]. *2014 Eleventh Annual IEEE International Conference on Sensing, Communication, and Networking* (*SECON*), IEEE, 2014: 293-301.

[10] 高玉威, 熊俊, 郭登科, 等. 面向无人机空地通信的无线信道密钥生成技术研究[J]. 密码学报, 2022, 9(1): 76-87.
GAO Y W, XIONG J, GUO D K, *et al*.. Design of key generation schemes for aerial communication scene of UAVs[J]. *Journal of Cryptologic Research*, 2022, 9(1): 76-87. (in Chinese).

[11] FURQAN H M, HAMAMREH J M, ARSLAN H. Secret key generation using channel quantization with SVD for reciprocal MIMO channels[C]. *2016 International Symposium on Wireless Communication Systems* (*ISWCS*), IEEE, 2016: 597-602.

[12] WALLACE J W, SHARMA R K. Automatic secret keys from reciprocal MIMO wireless channels: measurement and analysis[J]. *IEEE Transactions on Information Forensics and Security*, 2010, 5(3): 381-392.

[13] ZHAN F R, YAO N M, GAO ZH G, *et al*.. Efficient key generation leveraging wireless channel reciprocity for MANETs[J]. *Journal of Network and Computer Applications*, 2018, 103: 18-28.

[14] YANG L, GAO Y S, ZHANG J Q, *et al*.. A channel perceiving attack and the countermeasure on long-range IoT physical layer key generation[J]. *Computer Communications*, 2022, 191: 108-118.

[15] LU Y J, WU F, HUANG Q Y, *et al*.. Telling secrets in the light: an efficient key extraction mechanism via ambient light[J]. *IEEE Transactions on Wireless Communications*, 2021, 20(1): 186-198.

作者简介：

陈纯毅(1981—)，男，重庆人，博士，教授，博士生导师，主要从事无线光通信、大气光传输、物理层信息安全、虚拟现实等研究工作。E-mail: chenchunyi@hotmail.com