从毫米波到太赫兹的单输入单输出和多输入多输出连续变量量子密钥分发

Mingqi Zhang[1],*, Stefano Pirandola[2] 和 Kaveh Delfanazari[1]

[1] 格拉斯哥大学詹姆斯·瓦特工程学院电子与纳米工程部，英国格拉斯哥 G12 8QQ [2] 约克大学计算机科学系，英国约克 YO10 5GH*通讯作者：kaveh.delfanazari@glasgow.ac.uk日期：2022年12月25日

摘要—随着对大带宽的需求呈指数级增长，我们有必要考虑最佳网络平台，以及通信网络中信息的安全与隐私。人们提出采用高载波频率的毫米波（mm）和太赫兹（THz）作为关键技术，通过提供超宽带信号突破现有通信系统的香农信道容量极限。毫米波和太赫兹还能够构建与光通信系统兼容的无线链路。然而，在这些频段（100GHz–10THz）能够以较高效率运行的大多数固态元件，尤其是信号源和探测器，都需要低温冷却，这也是大多数量子系统的要求。在此，我们展示，当信号源和探测器在低至 T= 4K 的低温下运行时，可以实现安全的毫米波和太赫兹量子密钥分发。我们比较了单输入单输出（SISO）和多输入多输出（MIMO）连续变量太赫兹量子密钥分发（CVQKD）方案，发现频率范围在 f=100 GHz 至 1 THz 之间时可获得正密钥率。此外，我们发现，降低温度可以延长最大传输距离并提高密钥率；使用1024×1024 天线，在 f=100GHz、T=4K 时，最大安全通信距离可超过 5Km。我们的研究结果或有助于推动下一代安全无线通信系统和量子互联网的发展，其应用范围涵盖星际通信和深空通信，以及室内和短距离通信。

索引词— 毫米波（mm）波、太赫兹（THz）波、6G通信、量子密钥分发（QKD）、量子通信、低温系统、多输入多输出、单输入单输出，

I. 引言

随着无线通信的发展以及信息安全的快速进步，人们需要更高的载波频率和更多的频谱资源 [1, 2]。毫米波（mm）和太赫兹（THz）波 [3-6] 可提供超宽带和高速率通信，被认为是构建下一代（6G）通信系统的关键 [7-11]。毫米波和太赫兹频段位于成熟的微波和光波段之间，属于探索较少的区域 [12-16]。由于器件和电路效率低且不切实际，这些频率范围的电磁频谱中存在一段空白。近年来，电子、光子和基于等离激元的毫米波和太赫兹技术取得了发展，并通过展示高功率效率的信号源 [20-26], 天线 [27-31], 滤波器 [32-34], 波导 [29, 35-39], 调制器 [40-49], 和探测器[3, 49-52]，帮助弥合了这一空白。6G的需求包括但不限于太比特每秒（Tb/s）、毫米级精度的传感和定位、无缝连接以及超高速无线通信 [7-11]。此外，在低温（低温工程）下运行的量子处理器和量子计算机的实际应用 [53-55], 需要在高性能经典处理器、计算机和通信系统之间进行大规模开放空气和自由空间数据传输。因此，要实现实用量子信息处理的稳健构建模块，就应同时关注安全性和低温运行。与自由空间光链路相比，太赫兹链路在雾天条件等恶劣环境下更加稳定 [56]。毫米波 [57] 和太赫兹链路 [58, 59] 在长距离传输中的限制主要由空气吸收造成 [60]。因此，找到该频段内大气吸收较低的窗口非常重要。高等级安全性也是实现毫米波和太赫兹通信的重要方面，而采用经典密码方案来维持这种安全性颇具挑战。量子密钥分发（QKD）借助量子物理的力量，有助于实现高等级的无条件安全性 [61-64]。量子密钥分发可分为离散变量（基于单光子源和探测器的DVQKD）和连续变量（基于标准通信系统的CVQKD） [62-75]。CVQKD 采用相干零差探测，而不是单光子探测[65] ，并且可以与下一代通信系统集成 [66]。

单输入单输出（SISO）是一种经典通信系统，其发射机和接收机均不配备多根天线。为了满足数据传输量激增的需求，如今多输入多输出（MIMO）技术已广泛应用于无线通信。发射端和接收端均配备多根天线的MIMO系统，在带宽和发射功率有限的情况下，仍能提升数据吞吐量并扩大通信范围 [67]。文献 [61] 和 [68], 介绍了采用单输入单输出和多输入多输出系统的太赫兹量子密钥分发，主要关注中红外——

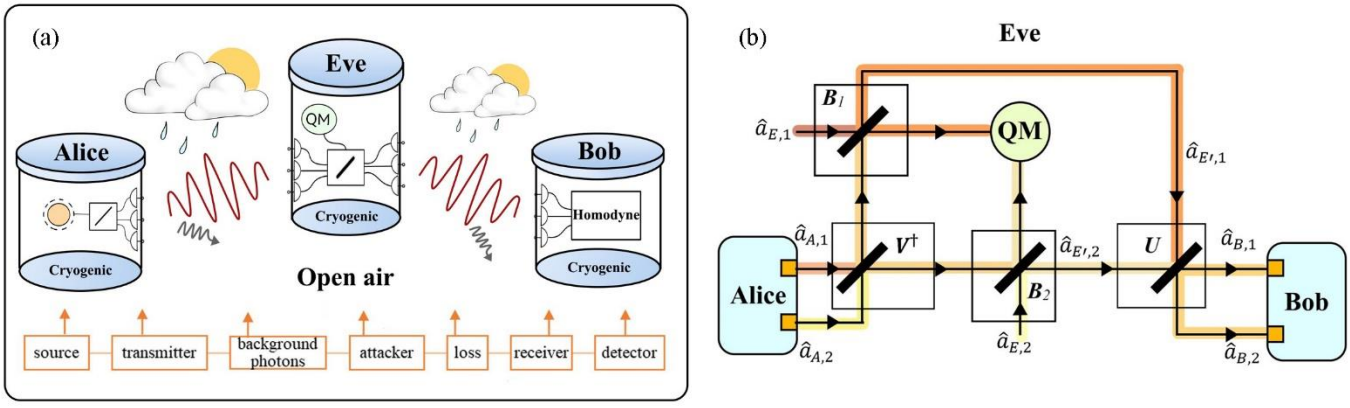

图1. (a) 所提出的毫米波和太赫兹量子密钥分发的系统模型。Alice 在源（即发生器）处制备热态。发射机和接收机是按一维均匀线性阵列（ULA）分布的天线。Alice、Bob 和 Eve 在低温环境中执行各自的操作。开放空气环境中的信道损耗包括大气吸收和自由空间损耗。Eve 的输出模式存储在量子存储器（QM）中。Bob 使用零差探测器测量正交分量。(b) 针对 2×2 多输入多输出系统所描述的移相器模型示意图。该信道由 4 个分束器建模。Alice 根据随机向量生成 2 个相干态 $\hat{a}_{A,1}$ 和 $\hat{a}_{A,2}$，并将它们作为热态从她的 2 根天线发射出去。这两个态由第一个分束器 $\boldsymbol{V}^{\dagger}$混合。随后，Eve 实施集体高斯攻击。她制备两个双模压缩真空态，并使用分束器 $\boldsymbol{B}_1$ 和 $\boldsymbol{B}_2$ 将输入与她的态混合。输出模式和其中一个原始模式被存储在量子存储器（QM）中。在 Bob 探测输入之前，信号由分束器 $\boldsymbol{U}$混合。 最后，Bob 使用他的两根天线接收模式 $\hat{a}_{B,1}$ 和 $\hat{a}_{B,2}$。

及远红外频段（10THz-40THz），且工作于室温（T= 296 K）。

受 [61] 和 [68], 相关研究的启发，本文聚焦于温度为 T < 50 K 时的单输入单输出和多输入多输出量子密钥分发。我们研究频率范围从 f=100 GHz 到 1 THz 的毫米波和太赫兹连续变量量子密钥分发，天线和探测器均在低温环境（T< 50 K）下运行。此外，我们比较了这一频率范围内单输入单输出和多输入多输出连续变量量子密钥分发系统的性能。

II. 系统模型

对于所提出的毫米波和太赫兹量子通信方案，低温天线会产生以角频率 ω 振荡的电磁（EM）场。该电磁场经过量子化后，系统得到哈密顿量 $H = \mathrm{h}\omega(\hat{a}^{\dagger}\hat{a} + \frac{1}{2})$。H 与量子谐振子的哈密顿量相似，其中 h 为普朗克常数，$\hat{a}$ 为湮灭算符，$\hat{a}^{\dagger}$ 为产生算符。此外，正交分量场算符 $\hat{\mathrm{q}} = \frac{\hat{a}+\hat{a}^{\dagger}}{\sqrt{2}}$ 和 $\hat{\mathrm{p}} = \frac{\mathrm{i}(\hat{a}+\hat{a}^{\dagger})}{\sqrt{2}}$ 是系统的无量纲正则可观测量（类似于量子谐振子的位置和动量）[69]。最后，系统的相干态是湮灭算符 $\hat{a}$的本征态，由 $\hat{a}|\alpha\rangle = \alpha|\alpha\rangle$给出。这里，$\alpha = \mathrm{q} + \mathrm{ip} \in \mathrm{C}$ 表示相干态振幅 [68], , 其取自二维高斯分布。两个相互独立的连续变量 q 和 p 用于在 Alice 与 Bob 之间生成密钥[61]。

符号说明：粗体斜体大写字母（如 A）表示矩阵。$\boldsymbol{A}^{\dagger}$ 表示矩阵 A 的共轭转置，$\boldsymbol{A}^{T}$ 表示转置。$\mathbf{0}_{M\times N} \in \mathrm{C}^{M\times N}$ 表示零复矩阵，并且 $\mathbf{1}_{M\times N} \in \mathrm{C}^{M\times N}$ 表示元素全为 1 的复矩阵。$\boldsymbol{I}_M$ 表示$M \times M$ 单位矩阵。由$diag(\boldsymbol{a})$描述的$M \times M$ 对角矩阵，其对角线上的元素为$\boldsymbol{a}$，记作$\boldsymbol{a} \in \mathrm{C}^{M}$。此外，$\mathcal{N}(\mu, \boldsymbol{\Sigma})$表示实多元高斯分布，其中向量为$\mu$，协方差矩阵（CM）为$\boldsymbol{\Sigma}$。

A. 信道模型

如图 1(a) 所示，我们考虑一个单向通信信道，以在 Alice 和 Bob 之间建立密钥。Alice 与 Bob 之间的多输入多输出毫米波和太赫兹通信信道包括：Alice 一侧配备 N_t 根天线的发射机，以及 Bob 一侧配备 N_r 根天线的接收机。我们假设两侧的天线均以一维均匀线性阵列（ULA）排列，且每个天线单元的增益为 G_a。因此，Alice 和 Bob 的天线增益分别为 $G_t = N_t G_a$ 和 $G_r = N_r G_a$ [68]。热态的高斯调制是一种广泛用于多种频率的编码协议 [61]。Alice 从真空态 $|0\rangle$ 开始，从 N_t 根天线生成振幅为 $a_i = Q_{A,i} + jP_{A,i},\ i = 1, 2, \ldots, N_t$ 的 N_t 个相干态 $|a_i\rangle$；其正交分量取自两个相互独立的随机向量 $\boldsymbol{Q}, \boldsymbol{P} \sim \mathcal{N}(\mathbf{0}_{N_t\times 1}, V_s \boldsymbol{I}_{N_t})$，其中 V_s 是初始信号编码 [68] 的方差。Alice 的第 i 个天线单元随机发送量子太赫兹源（热）态的两个正交分量 $\hat{Q}_{A,i}$ 和 $\hat{P}_{A,i}$，并用 $\hat{X}_{A,i} \in \{\hat{Q}_{A,i}, \hat{P}_{A,i}\}$ 描述。因此，Alice 的第 i 个模式可表示为 $\hat{X}_{A,i} = a_i + \hat{0}$，其中 $\hat{0}$ 是由毫米波和太赫兹背景热噪声引起的热模式（正交分量算符），$\mathrm{X_{Ai}}$ 表示经典调制变量 [61, 76]。Alice 模式的总方差为

$$V_a = V_s + V_0 \qquad (1)$$

其中，V_0 为方差（包含真空模式的方差和制备噪声的方差）[61]。V_0 定义为

$$V_0 = 1 + 2\bar{n} \quad (2)$$

这里，1为真空的散粒噪声单位（shot noise unit），且

$$\bar{n} = \left[\exp\left(\frac{hf_c}{k_B T}\right) - 1\right]^{-1} \quad (3)$$

是平均热态，h 是普朗克常数，k_B 表示玻尔兹曼常数，T 是环境温度，f_c 是载波频率。现在，考虑 Alice 通过不安全的量子信道将她的状态发送给 Bob（接收机）。Bob 使用有噪声零差检测技术，该技术基于毫米波和太赫兹散粒噪声极限量子探测器，并在正交分量 $\hat{Q}$ 和 $\hat{P}$ 之间随机切换，以测量传入的热态。

Alice 与 Bob 之间的信道矩阵可建模为 [68, 70, 71]

$$\boldsymbol{H} = \sum_{l=1}^{L} \sqrt{\gamma_l} e^{j2\pi f_c \tau_l} \psi_{N_r}(\phi_{r,LOS}) \psi_{N_t}^{\dagger}(\phi_{t,LOS}) \quad (4)$$

其中，$\boldsymbol{H} \in \mathbb{C}^{N_r \times N_t}$，$\tau_l$ 是第 l 条多径的传播时延。本研究仅考虑视距路径（LOS），其中 L=1 。因此，路径损耗 γ_l 表示为 [68]

$$\gamma_{l=1} = G_t G_r \left(\frac{\lambda}{4\pi d}\right)^2 10^{-\frac{\delta d}{10}} \quad (5)$$

其中，d 是 Alice 与 Bob 之间的距离，δ 是大气损耗，定义为 dB/km [61, 70]。它包含毫米波和太赫兹波的自由空间路径损耗及大气吸收损耗。$\phi_{r,\,LOS}$ 和 $\phi_{t,\,LOS}$ 分别是 Bob 观测到的到达角和 Alice 的出发角。$\psi_K(\theta)$ 表示均匀线性阵列的阵列响应向量，该阵列包含 K 根天线。

信道模型的推导细节采用参考文献[68] 提出的奇异值分解（SVD）方案，详见附录A。

尽管相干攻击属于一般攻击，但参考文献[72, 73] 中的研究证明，只要系统能够抵御集体攻击，在密钥足够长时，也能够抵御一般攻击。在连续变量量子密钥分发中，针对高斯协议，最现实且研究最广泛的集体攻击是纠缠克隆攻击[61]。因此，我们假设信道完全由Eve控制，且她使用纠缠克隆器窃取信息。图1（b）以2 × 2 多输入多输出系统为例，该系统由4个分束器构成 [69]。Alice传输的两个模式经分束器$\boldsymbol{V}^{\dagger}$合并后，Eve会取出产生的两个输出模式。Eve应预先制备两对纠缠的爱因斯坦–波多尔斯基–罗森态$\{\hat{e}_1, \hat{E}_1\}$和$\{\hat{e}_2, \hat{E}_2\}$（也称为双模压缩真空态）。收到输入后，Eve使用$\boldsymbol{B}_1$ 和$\boldsymbol{B}_2$ 将它们与$\hat{E}_1$ 和$\hat{E}_2$合并。$\boldsymbol{B}$ 的输入与输出之间的关系可写为[68, 69]

$$\begin{bmatrix} \hat{a}_{out,1} \\ \hat{a}_{out,2} \end{bmatrix} = \begin{bmatrix} \sqrt{\eta_i} & \sqrt{1-\eta_i} \\ -\sqrt{1-\eta_i} & \sqrt{\eta_i} \end{bmatrix} \begin{bmatrix} \hat{a}_{in,1} \\ \hat{a}_{in,2} \end{bmatrix} \quad (6)$$

此处，η_i 是第 i 个分束器的一个输出（$\hat{E}'_1$、$\hat{E}'_2$）以及原始模式（$\hat{e}_1$、$\hat{e}_2$）存入她的量子存储器（QM）中，并测量辅助模式，以便在 Alice 和 Bob 完成经典通信后获取信息。另两个输出模式将被分束器$\boldsymbol{U}$ 合并后发送给 Bob。我们假设 Alice 在其一端采用$\boldsymbol{V}$ 作为波束成形的基础，而 Bob 在其一端采用$\boldsymbol{U}^{\dagger}$ 作为解码的基础。整个模型可由[68, 69]描述

$$\hat{\boldsymbol{a}}_B = \boldsymbol{U}^{\dagger}\boldsymbol{H}\boldsymbol{V}\hat{\boldsymbol{a}}_A + \boldsymbol{U}^{\dagger}\boldsymbol{U}\boldsymbol{S}\hat{\boldsymbol{a}}_E \quad (7)$$

其中 $\hat{\boldsymbol{a}}_B = [\hat{a}_{B,1}, \ldots, \hat{a}_{B,N_r}]$ 是 Bob 的接收模式，$\hat{\boldsymbol{a}}_A = [\hat{a}_{A,1}, \ldots, \hat{a}_{A,N_t}]^T$ 是 Alice 发送的模式，$\hat{\boldsymbol{a}}_E = [\hat{a}_{E,1}, \ldots, \hat{a}_{E,N_t}]^T$ 是 Eve 注入的高斯模式。

$$\boldsymbol{S} = diag\left\{\sqrt{1-\eta_1}, \ldots, \sqrt{1-\eta_r}, \boldsymbol{1}_{(M-r)\times 1}\right\} \quad (8)$$

是一个 $M \times M$ 对角矩阵，其中 $M = \min(N_t, N_r)$，详细信息见附录A。利用 H 的奇异值分解，可将 Alice 与 Bob 之间的有效信道分解为 r 个并行 SISO 信道（r 是 $\boldsymbol{H}$ 的秩）。在这种情况下，信道输入与输出之间的关系可写为 [68]

$$\hat{\boldsymbol{a}}_{B,i} = \sqrt{T_i}\hat{\boldsymbol{a}}_{A,i} + \sqrt{1-T_i}\hat{\boldsymbol{a}}_{E,i}, \qquad i = 1,2,\ldots,r \quad (9)$$

Here, T_i is the i-th non-zero eigenvalue of $\boldsymbol{H}^{\dagger}\boldsymbol{H}$ and $\hat{a}_{B,i}$ 也可视为信道的第 i 个透射率。对于每个接收到的 r 模式，Bob 都会随机选取一个正交分量进行零差实验，并得到附录A中详述的结果。

我们将 W 设为 Eve 引入的热噪声方差。因此，Bob 接收到的第 i 个模式的散粒噪声水平为$V(\hat{X}_{B,\,i}) = T_i V_0 + (1 - T_i)W$ [61]。$\hat{X}_{B,\,i}$ 是附录A中由式（22）描述的 Bob 接收的正交分量。如果 Eve 想要完全隐藏在背景噪声中，可以使用 $W = V_0$。这样，Bob 接收到的散粒噪声水平为 $V(\hat{X}_{B,\,i}) = V_0$，与 Alice 发送的相同。虽然低于 1THz 的频率可以使 V_0 的值增大，但我们可以通过将系统冷却至低温来获得$V_0 \approx 1\ SNU$。

B. 密钥率

在这一毫米波和太赫兹连续变量量子密钥分发方案中，Alice 和 Bob 多次重复先前的量子通信协议，以生成一个字符串。随后，他们使用协调协议纠正字符串中的错误。直接协调（DR）是指 Bob 使用 Alice 的编码字符串来生成密钥；反向协调（RR）则是指 Alice 根据 Bob 的解码结果生成密钥。Alice 和 Bob 使用协调协议进行隐私放大，以减少 Eve 窃取的信息量 [68]。在本研究中，我们采用渐近密钥率来研究毫米波和太赫兹量子密钥分发中 RR 协议的性能。在 RR 中，即使信道透射率接近 0，也有可能实现正密钥率；而在 DR 中，信道透射率必须大于 0。5 [76], 由于损耗很高（包括大气吸收和路径损耗），这种方案在毫米波和太赫兹频段并不实用。

根据[68], , MIMO系统的密钥率可分为 r 个单输入单输出信道。因此，我们首先分析单输入单输出信道的密钥率。在反向协调方案中，Alice 和 Bob 使用 Bob 端的解码结果生成密钥[74]。Alice 和 Bob 可以估算双方共享的互信息，表示为 $I(a:b)$，以及 Eve 的可访问信息，表示为 $I(E:b)$。渐近密钥率$R^{\leftarrow}$可用 Alice 和 Bob 共享的剩余信息来表示，其公式为 [62]

$$R^{\leftarrow} = I(a:b) - I(E:b) \quad (10)$$

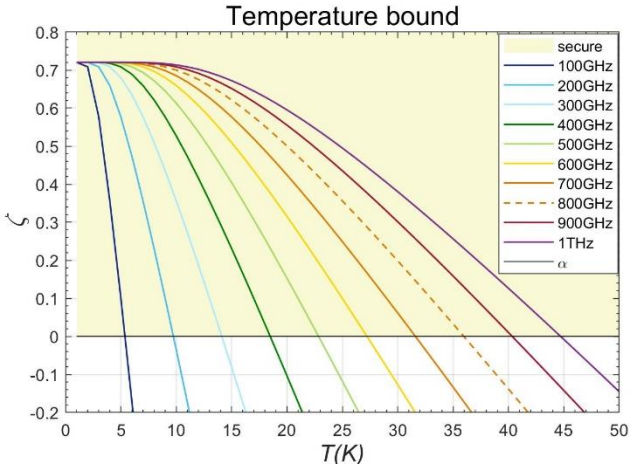

图 2。 曲线显示 ζ 不同频率下随温度变化的情况。为实现安全传输，ζ 应保持在直线 α （位于安全范围内）。

Alice 和 Bob 之间的互信息为

$$\mathrm{I(a:b)} = \frac{1}{2} log_2[1 + \frac{TV_s}{\Lambda(V_0, W)}] \quad (11)$$

$$\Lambda(\mathrm{x,y}) = \mathrm{Tx} + (1 - \mathrm{T})\mathrm{y} \quad (12)$$

而 $V_s \gg V_0$、W，Eve 的信息则由 Holevo信息 I E: b 限定，其定义为

$$\mathrm{I(E:b)} = H_E - H_{E|b} \quad (13)$$

其中，H_E 和 $H_{E|b}$ 分别是 Eve 的总状态和条件状态的冯·诺依曼熵，由附录A中的式 (25) 和式 (26) 给出 [68, 75]。

最终，总密钥率为 r 条单输入单输出链路的密钥率之和 [68]，假设 $T_i \to 0$

$$R_{MIMO}^{\rightarrow} = \sum_{i=1}^{r} R_i^{\rightarrow} \approx \zeta tr(\boldsymbol{H}^{\dagger}\boldsymbol{H}) - rh(W) \quad (14)$$

其中

$$\zeta = 0.72\left[\frac{V_s}{W} - \ln\left(\frac{V_a + 1}{V_a - 1}\right)\left(\frac{V_a^2 - W^2}{2W} - V_a\right)\right] \quad (15)$$

且 $tr(\boldsymbol{H}\ \dot{\boldsymbol{H}}) = \sum_{i=1}^{r} T_i \mathrm{h}(W)$ is a function given by

$$\mathrm{h(x)} = \frac{x+1}{2} log_2\left(\frac{x+1}{2}\right) - \frac{x-1}{2} log_2\left(\frac{x-1}{2}\right) \quad (16)$$

C. 系统条件

要获得正的密钥率，需要满足 $\zeta tr(\boldsymbol{H}^{\dagger}\boldsymbol{H}) > r\mathrm{h}(W)$。根据式 (1)–(4) 可知，只有式 (14) 中的 $\zeta tr(\boldsymbol{H}^{\dagger}\boldsymbol{H})$ 取决于频率，而 ζ 也取决于温度。在频率给定时，降低温度会使式 (15) 中的 V_0 减小、ζ 增大。温度给定而频率升高时，也会出现这种情况。但频率升高通常会带来更大的路径损耗，进而可能使 $tr(\boldsymbol{H}^{\dagger}\boldsymbol{H})$ 降低。由于 tr $\overline{tr\ \boldsymbol{H}\ \boldsymbol{H}}$ $\zeta >$ ($\alpha = 0$ $^{=1}{}_{r}$ $\mathrm{h}(W)$ (+) $\boldsymbol{H}^{\dagger}\boldsymbol{H}$)>0，$\zeta > \alpha =$ 的极限等于 while W。该条件有助于我们在 ζ 与 $tr(\boldsymbol{H}^{\dagger}\boldsymbol{H})$ 之间找到平衡，从而获得正的密钥率。

图2展示了多输入多输出太赫兹量子密钥分发系统 [68] 中不同频率下 ζ 随温度的变化关系。根据仿真结果，在温度 T<43K 时，我们实现了频率范围为 f=100GHz 至 1THz 的安全传输。各频率对应的最高工作温度详情见表1。

III. 仿真结果

我们使用密钥率 (R) 来判断系统是否安全。正的密钥率表示传输安全。由于 MIMO系统的 R 是 SISO系统的总和，我们还比较了相同条件下 MIMO 和 SISO 系统的不同性能。

表 I

频率	大气吸收 δ	最高温度 T_{max} (K)	32×32的距离 温度为 T_{max} (m) 的MIMO系统
100GHz	0.4dB/km	4	700
200GHz	3dB/km	8	320
300GHz	4dB/km	13	75
400GHz	20dB/km	17	86
500GHz	50dB/km	21	68
600GHz	150dB/km	26	26
700GHz	70dB/km	30	38
800GHz	100dB/km	35	36
900GHz	100dB/km	39	25
1THz	100dB/km	43	21

A. MIMO系统的仿真

根据[60], [77], [78], , 各频率的大气吸收如表1所示。我们假设目标为
密钥率为10^{-5} bit/use [68]。表1还展示了32×32 多输入多输出系统在各频率下的最高温度对应的距离。虽然 f=700GHz 和 f=800GHz 可以达到

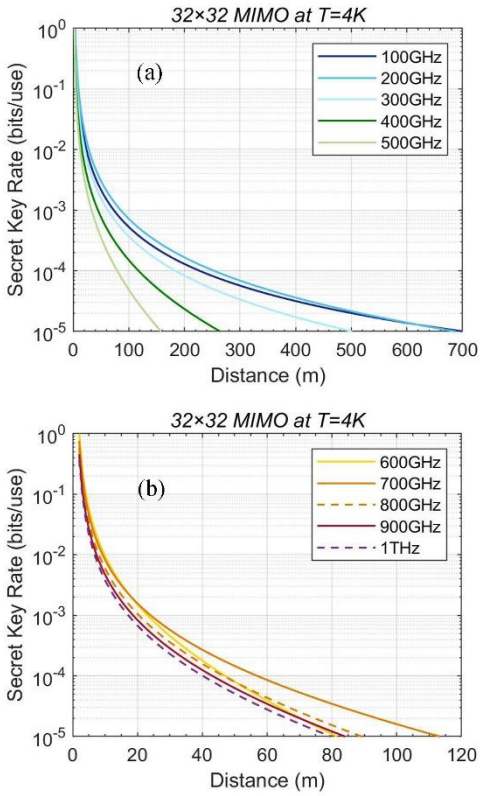

图3. (a) 在f=100GHz至500GHz、T=4K条件下，32×32 MIMO系统的传输距离。(b) 在f=600GHz至1THz、T=4K条件下， 32×32 MIMO系统的传输距离。此处参数为G_a=30、W=1、V_a=1000。

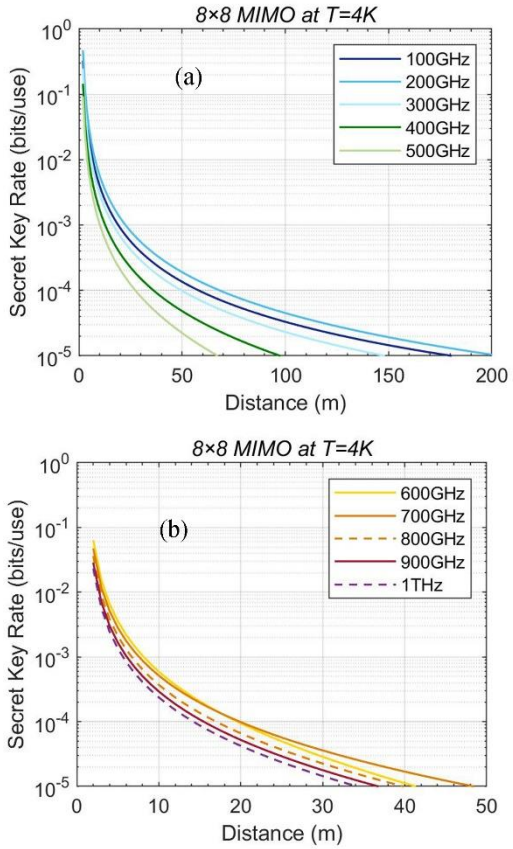

图 4. (a) 在 T=4K 下， 8×8 多输入多输出系统从 f =100GHz 到 500GHz 的传输距离。(b) 在 T=4K 下， 8×8 多输入多输出系统从 f=600GHz 到 1THz 的传输距离。此处，参数为 G_a=30、W=1、V_a=1000。

在 T>30K 时超过 35m，但由于该频率下吸收更强，f=600 GHz 在较低温度下只能达到 26m。图3展示了在 T=4K 时，32×32 多输入多输出系统中频率从 f=100GHz 到 1THz 范围内，密钥率随安全传输距离的变化情况。f=100GHz 和 f=200 GHz 的距离在 T=4K 时可达到 d=700m，这是所有频率中可达到的最大值。f=300GHz 的安全距离可达 d=500m，但频率高于 f=500GHz 时将降至 d=160m 以下。如果数量天线数量减少到 8×8 时，如图 4（a）所示，f=200GHz 时的最大距离仍可达到 d=200m。但对于图 4（b）中高于 f=600GHz 的频率，由于吸收较强，距离均低于 50m。

如图 5 所示，高阶多输入多输出配置可以提高最大安全距离。对于一个 32×32 多输入多输出系统，最大距离为 d=700m；而如图 5（a）所示，在 f=100GHz、T=4K 条件下， 1024×1024多输入多输出系统的安全传输距离可远超 d=8000m。f=200GHz、T =8K 以及 f=1THz、T=43K 条件下也呈现相同趋势。对于 f=200 GHz，在 T=8K 条件下，1024×1024 多输入多输出系统的最大距离超过 d=3000m。但在 f=1THz、T=43K 条件下，安全距离并没有短得那么多，这是因为大气吸收和热噪声导致的信道损耗较高。在 T=43K 条件下， 1024×1024多输入多输出天线系统的距离仅能达到 160m。与图 3（b）相比，在 f=1THz、T=43K 条件下，使用 32×32 根天线时的距离仅为 T=4K 条件下的五分之一。

B. 单输入单输出系统的仿真

与大型多输入多输出方案相比，在频率范围 f=100 GHz 至 f=1THz 内，单输入单输出方案的最大距离较短。假设目标密钥率为 10^{-5} bit/use [68]。图 6 (a) 显示，在 T=8K 时，频率为 f=200GHz 的单输入单输出系统最大距离小于 12m，远小于图 5 (b) 所示多输入多输出系统中的最大距离。图 6 (b) 显示了在 T= 4K 时，单输入单输出方案在 f=100GHz 至 1THz 范围内的距离。我们可以发现，在 200GHz 至 1THz 范围内，最大距离会随频率升高而减小，这是由路径损耗造成的。比较图 6 (a) 和 (b) 可明显看出，在相同频率下，较低的温度会增加最大距离。

比较图 6(b)与图 4可知，在相同温度下，多输入多输出方案能够实现比单输入单输出方案更远的距离。因此，在毫米波和太赫兹量子密钥分发系统中使用多根天线是必要的。由于频率为 f=800GHz、f=900GHz 和 f=1THz 时的大气吸收相同，图 6(b)显示，较低频率可提高传输距离。这可能是因为，较低频率下自由空间路径损耗较小，其影响超过了V_0 的增加（进而使=800降低）；而tr（$\boldsymbol{H}^{\dagger}\boldsymbol{H}$）的增加

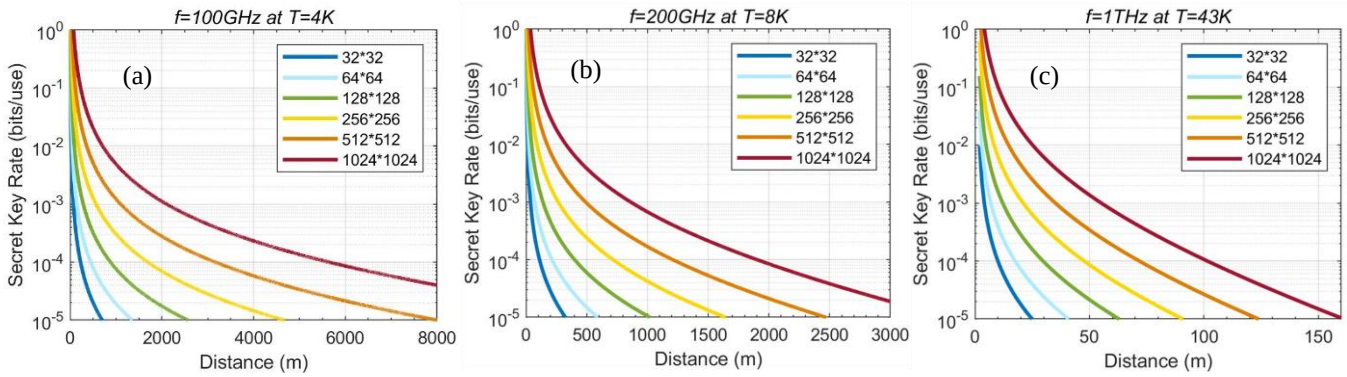

图 5. 曲线展示了 MIMO系统中不同天线数量对应的密钥率随传输距离的变化关系。(a) 为f=100GHz、T=4K时的结果。(b) 为f=200GHz、T=8K时的结果。(c) 为f=1THz、T=43K时的结果。

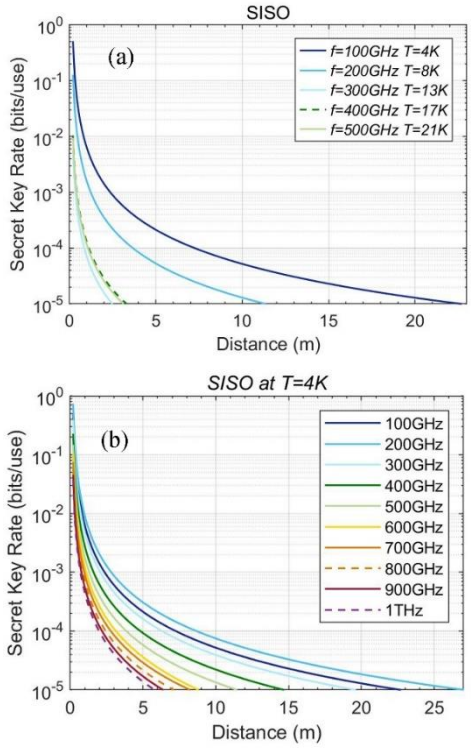

图 6. (a) 最高工作温度下，单输入单输出（SISO）的密钥率 R 随传输距离变化的关系，频率范围为*f*=100GHz 至*f* =500GHz。信道中的大气吸收见表1。(b) 在*T*=4K 下，单输入单输出（SISO）的密钥率 R 随传输距离变化的关系，频率范围为*f*=100GHz 至*f*=1THz。

在该范围内会使ζ降低。因此，要增大安全距离，可以使用更多天线、降低温度或选择较低的频率。

IV. 结论

在本研究中，我们研究了毫米波和太赫兹频段（从 f = 0.1 到 f= 1THz）的单输入单输出和多输入多输出量子密钥分发方案，并采用了信号源和探测器低温运行。我们发现，在目标频段内可以实现正的密钥率。与单输入单输出方案相比，多输入多输出技术能够提升安全传输距离。此外，我们还表明，系统中的天线越多，可实现的传输距离就越远。要构建长距离安全通信信道，需要更多天线、较低的工作温度和更低的频率。本研究假设分束器和通信信道具有理想性能；然而，要通过实际硬件实现完整方案，仍需开展大量研究工作。

参考文献

[1] T. Nagatsuma 等人，《基于光子技术的太赫兹无线通信》，Optics Express，第 21 卷，第 20 期，第 23736–23747 页，2013 年。

[2] D. M. M. Thomas Kürner、Tadao Nagatsuma，《太赫兹通信：迈向无线 Tbps》。Springer，ISBN：978-3-030-73738-2。

[3] K. Delfanazari、R. A. Klemm、H. J. Joyce、D. A. Ritchie 和 K. Kadowaki，《基于层状超导体的集成式、便携式、可调谐相干太赫兹信号源与高灵敏度探测器》，Proceedings of the IEEE，第 108 卷，第 5 期，第 721–734 页，2020年。

[4] H. Elayan、O. Amin、R. M. Shubair 和 M. S. Alouini，“太赫兹通信：5G 之后无线技术的发展机遇”，载于《2018年国际先进通信技术与网络会议》（CommNet），2018年4月2—4日，2018年，第1—5页，doi：10.1109/COMMNET.2018.8360286。

[5] K. Kadowaki 等，“利用高温超导 $Bi_2Sr_2CaCu_2O_{8+\delta}$ 本征约瑟夫森结产生的相干辐射实现量子太赫兹电子学（QTE）”，Physica C: Superconductivity，第 491 卷，第 2–6 页，2013 年。

[6] M. J. Fitch 和 R. Osiander，“用于通信和传感的太赫兹波”，JOHNS HOPKINS APL TECHNICAL DIGEST，第 25 卷，第 4 期，第 348–355 页，2004 年。

[7] Z. T. Ma、Z. X. Geng、Z. Y. Fan、J. Liu 和 H. D. Chen，“太赫兹通信调制器：当前技术水平”，Research，第 2019 卷，2019年。

[8] Z. Chen 等，“太赫兹通信综述”，China Communications，第 16 卷，第 2 期，第 1–35 页，2019年。

[9] Z. Chen 等，《面向2030年及以后的太赫兹无线通信：前沿技术》，IEEE Communications Magazine，第59卷，第11期，第66–72页，2021年。

[10] H. Sarieddeen、M. S. Alouini 和 T. Y. Al-Naffouri，《太赫兹通信信号处理技术概述》，Proceedings of the IEEE，第109卷，第10期，第1628–1665页，2021年。

[11] H. J. Song 和 T. Nagatsuma，《太赫兹通信的现状与未来》，IEEE Transactions on Terahertz Science and Technology，第1卷，第1期，第256–263页，2011年。

[12] M. Tsujimoto 等，《超导 $Bi_2Sr_2CaCu_2O_{8+\delta}$ 单晶电流-电压特性内部支路产生的宽范围可调亚太赫兹辐射》，Physical Review Letters，第108卷，第10期，2012年。

[13] K. Delfanazari 等，《基于高温超导体本征约瑟夫森结的太赫兹振荡器件》，Journal of Infrared Millimeter and Terahertz Waves，第 35 卷，第 1 期，第 131-146 页，2014 年。

[14] I. F. Akyildiz、C. Han、Z. Hu、S. Nie 和 J. M. Jornet，《太赫兹频段通信：重新审视一个老问题及未来十年的研究方向》，IEEE Transactions on Communications，第 70 卷，第 6 期，第 4250-4285 页，2022年。

[15] K. Delfanazari 等，《用于从超导 $Bi_2Sr_2CaCu_2O_{8+\delta}$ 本征约瑟夫森结产生太赫兹波辐射的多种几何形状台面结构的实验与理论研究》，载于第37届红外、毫米波和太赫兹波国际会议（IRMMW-THz），卧龙岗大学，卧龙岗，澳大利亚，2012年9月23日至28日；载于红外、毫米波和太赫兹波国际会议，2012年。

[16] R. H. Caverly，《微波领域的突破：可编程太赫兹芯片级表面与系统——访谈 Kaushik Sengupta博士》，IEEE Journal of Microwaves，第1卷，第4期，第853-863页，2021年。

[17] K. Delfanazari 等，《尖锐等腰三角形 $Bi_2Sr_2CaCu_2O_{8+\delta}$ 台面结构中本征约瑟夫森结的可调太赫兹发射》，Optics Express，第21卷，第2期，第2171-2184页，2013年。

[18] T. Kashiwagi 等，《高温超导太赫兹发射器：基础物理及其应用》，Japanese Journal of Applied Physics，第51卷，第1期，2012年。

[19] T. Kashiwagi 等，《高效制备自热效应大幅降低的本征约瑟夫森结太赫兹振荡器》，Physical Review Applied，第4卷，第5期，2015年。

[20] T. Kashiwagi 等人，“不同厚度 $Bi_2Sr_2CaCu_2O_{8+\delta}$ 晶体中本征约瑟夫森结太赫兹发射器的辐射特性研究”，Materials，第 14 卷，第 5 期，doi：10.3390/ma14051135。

[21] K. Delfanazari 等人，“偏置电极位置对超导 $Bi_2Sr_2CaCu_2O_{8+\delta}$ 五边形台面结构太赫兹辐射的影响”，IEEE Transactions on Terahertz Science and Technology，第 5 卷，第 3 期，第 505-511 页，2015年。

[22] Y. Xiong、T. Kashiwagi、R. A. Klemm、K. Kadowaki 和 K. Delfanazari，《集成超导相干太赫兹发射器中的腔模与偏振设计》，载于2020年

第45届红外、毫米波和太赫兹国际会议（IRMMW-THz），2020年11月8日至13日，2020年，第1-2页，doi: 10.1109/IRMMW-THz46771.2020.9370587.[23] K. Delfanazari 等，《超导 $Bi_2Sr_2CaCu_2O_{8+\delta}$ 本征约瑟夫森结等边三角形台面中的相干连续太赫兹波发射研究》，Physica C- Superconductivity and Its Applications，第491卷，第16-19页，2013年。[24] Y. Saiwai 等，《无液氦高温超导太赫兹发射系统及其应用》，Japanese Journal of Applied Physics，第59卷，第10期，页码105004，2020年。[25] K. A. Fedorova 等，《宽调谐太赫兹半导体盘式激光器》，physica status solidi (RRL) – Rapid Research Letters，第14卷，第10期，页码2000204，2020年。[26] R. Cattaneo、E. A. Borodianskyi、A. A. Kalenyuk 和 V. M. Krasnov，《功率效率达12%的超导太赫兹源》，Physical Review Applied，第16卷，第6期，2021年。[27] J. R. Rain 等，《高对称性薄型微带天线与二维量子盒的波函数》，Physical Review A，第104卷，第6期，页码062205，2021年。[28] Y. Xiong 和 K. Delfanazari，《芯片集成高温超导太赫兹天线中的圆偏振设计》，载于2021年光子学与电磁学研究研讨会（PIERS），2021年11月21日至25日，2021年，第1016-1019页，doi: 10.1109/PIERS53385.2021.9694960。[29] Y. Xie、N. Bai、W. Hong 和 X. Sun，《用于 G 波段行波管的六角晶格缺陷光子晶体波导慢波结构研究》，Journal of Electromagnetic Waves and Applications，第36卷，第6期，第843-855页，2022年。[30] D. P. Cerkoney 等，《高温超导体 $Bi_2Sr_2CaCu_2O_{8+\delta}$等边三角形微带天线的太赫兹发射腔模增强》，Journal of Physics: Condensed Matter，第29卷，第1期，页码015601，2017年。[31] R. A. Klemm 等，《三角形 $Bi_2Sr_2CaCu_2O_{8+\delta}$ 台面太赫兹发射的电磁腔模贡献建模》，Physica C: Superconductivity，第491卷，第30-34页，2013年。[32] S. Kalhor、M. Ghanaatshoar 和 K. Delfanazari，《片上超导太赫兹超材料带通滤波器》，载于2020年第45届红外、毫米波和太赫兹国际会议（IRMMW-THz），2020年11月8日至13日，2020年，第1-2页，doi: 10.1109/IRMMW-THz46771.2020.9370663。[33] K. Yang、S. Liu、S. Arezoomandan、A. Nahata 和 B. Sensale-Rodriguez，《石墨烯基可调超材料太赫兹滤波器》，Applied Physics Letters，第105卷，第9期，页码093105，2014年。[34] I. J. H. McCrindle、J. Grant、T. D. Drysdale 和 D. R. S. Cumming，《多光谱材料：光学等离激元滤波器与太赫兹超材料吸收器的混合》，Advanced Optical Materials，第2卷，第2期，第149-153页，2014年。[35] S. Kalhor、M. Ghanaatshoar、H. J. Joyce、D. A. Ritchie、K. Kadowaki 和 K. Delfanazari，《用于低温集成纳米光子学的毫米波至太赫兹超导等离激元波导》，Materials，第14卷，第15期，2021年。[36] S. Atakaramians、S. Afshar V、T. M. Monro 和 D. Abbott，《太赫兹介质波导》，Advances in Optics and Photonics，第5卷，第2期，第169-215页，2013年。[37] S. Kalhor、M. Ghanaatshoar 和 K. Delfanazari，《超导纳米电路中的太赫兹光子导引》，载于2020年中英新兴技术国际会议（UCET），2020年8月20日至21日，2020年，第1-3页，doi: 10.1109/UCET51115.2020.9205480。[38] G. Gallot、S. P. Jamison、R. W. McGowan 和 D. Grischkowsky，《太赫兹波导》，J. Opt. Soc. Am. B，第17卷，第5期，第851-863页，2000年。[39] K. Wang 和 D. M. Mittleman，《用于太赫兹波导引的金属线》，Nature，第432卷，第7015期，第376-379页，2004年。[40] S. Kalhor、M. Ghanaatshoar、T. Kashiwagi、K. Kadowaki、M. J. Kelly 和 K. Delfanazari，《高温超导 $Bi_2Sr_2CaCu_2O_{8+\delta}$ 太赫兹超材料的热调谐》，IEEE Photonics Journal，第9卷，第5期，2017年。[41] R. Degl'Innocenti、H. Lin 和 M. Navarro-Cía，《太赫兹超材料调制器的最新进展》，第11卷，第8期，第1485-1514页，2022年。[42] V. Savinov、K. Delfanazari、V. A. Fedotov 和 N. I. Zheludev，《超导亚太赫兹中的巨大非线性超材料，" Applied Physics Letters，第108卷，第10期，页码101107，2016年。

[43] A. S. Malishevskii 和 S. A. Uryupin，"约瑟夫森夹层中涡旋对电磁波的切伦科夫激发"，《物理学文稿》，第97卷，第5期，页码055817，2022年。

[44] S. Kalhor 等，"采用混合石墨烯-超导体光子集成电路的有源太赫兹调制器与慢光超材料器件"，《纳米材料》，第11卷，第11期，2021年。

[45] A. Squires、X. Gao、T. van der Laan、Z. Han 和 J. Du，"利用石墨烯薄膜为太赫兹超表面添加可调响应"，《红外、毫米波与太赫兹波杂志》，第43卷，第9期，806–818页，2022年。

[46] S. Kalhor 等人，"采用石墨烯-超导体混合耦合开口环谐振器阵列的有源太赫兹调制器与慢光超材料器件"，载于 2022年光子学与电磁学研究研讨会（PIERS），2022年4月25日至29日，第967-971页，doi：10.1109/PIERS55526.2022.9792980。

[47] S. J. Kindness 等人，"一种太赫兹手性超材料调制器"，Advanced Optical Materials，第8卷，第21期，第2000581页，2020年。

[48] C. Li 等人，"基于超导复合结构超材料的电控太赫兹开关器件"，Applied Physics Letters，第121卷，第3期，第031702页，2022年。

[49] S. J. Kindness 等人，"用于太赫兹量子级联激光器全电控偏振控制的石墨烯集成超材料器件"，《ACS光子学》，第6卷，第6期，第1547-1555页，2019年。

[50] F. Sizov 和 A. Rogalski，《太赫兹探测器》，《量子电子学进展》，第 34 卷，第 5 期，第 278-347 页，2010 年。

[51] S. Castilla 等人，《利用天线集成石墨烯 pn 结实现快速、灵敏的太赫兹探测》，《纳米快报》，第 19 卷，第 5 期，第 2765-2773 页，2019 年。

[52] R. A. Lewis，《太赫兹探测器综述》，《物理学杂志D：应用物理》，第 52 卷，第 43 期，第 433001 页，2019 年。

[53] M. Zhang、Foshat, P.、Poorgholam Khanjari, S.、Imran, M.、Weides, M. 和 Delfanazari, K，《采用低温微波组件的超导量子计算微波量子密钥分发》，发表于2022年量子计算国际研讨会：电路、系统、自动化与应用（QC-CSAA），美国田纳西州诺克斯维尔，2022年7月18日至19日。

[54] P. Magnard 等，"空间分离的低温系统中超导电路之间的微波量子链路"，Physical Review Letters，第 125 卷，第 26 期，第 260502 页，2020年。

[55] F. K. Florian Fesquet、Michael Renger、Qiming Chen、Kedar Honasoge、Oscar Gargiulo、Yuki Nojiri、Achim Marx、Frank Deppe、Rudolf Gross、Kirill G. Fedorov，"开放空间微波量子密钥分发的展望"，arXiv:2203.05530。

[56] Y. H. Yang、M. Mandehgar 和 D. R. Grischkowsky，"宽带太赫兹信号可穿透浓雾"，《IEEE光子技术快报》，第 27 卷，第 4 期，第 383-386 页，2015年。

[57] M. Karmoose、C. Fragouli、S. Diggavi、R. Misoczki、L. L. Yang 和 Z. L. Zhang，"利用毫米波建立密钥"，IEEE Communications Letters，第 23 卷，第 6 期，第 1077-1080 页，2019年。

[58] Z. Q. Wang、R. Malaney 和 J. Green，《太赫兹频率下的星间量子密钥分发》，载于 IEEE 国际通信大会（IEEE ICC），中华人民共和国上海，2019年5月20日至24日，IEEE 国际通信大会，2019年。

[59] Y. Q. He、Y. Y. Mao、D. Huang、Q. Liao 和 Y. Guo，《太赫兹频段连续变量量子密钥分发的室内信道建模》，Optics Express，第 28 卷，第 22 期，第 32386-32402 页，2020年。

[60] T. Schneider、A. Wiatrek、S. Preussler、M. Grigat 和 R. P. Braun，《太赫兹固定无线链路的链路预算分析》，IEEE Transactions on Terahertz Science and Technology，第 2 卷，第 2 期，第 250-256 页，2012年。

[61] C. Ottaviani 等，《太赫兹量子密码学》，《IEEE通信领域精选期刊》，第 38 卷第 3 期，页码 483-495，2020年。

[62] S. Pirandola 等，《量子密码学进展》，Advances in Optics and Photonics，第 12 卷第 4 期，页码 1012-1236，2020年。

[63] S. Pirandola、R. Laurenza、C. Ottaviani 和 L. Banchi，《无中继量子通信的基本极限》，《自然·通讯》，第 8 卷，2017年。

[64] S. Pirandola，《连续变量量子密钥分发的可组合安全性：信任级别和实际密钥率，适用于

有线和无线网络》，Physical Review Research，第3卷，第4期，043014页，2021年。[65] I. H. L. Grande、S. Etcheverry、J. Aldama、S. Ghasemi、D. Nolan 和 V. Pruneri，《用于离散变量和连续变量量子密钥分发的自适应发射机》，Optics Express，第29卷，第10期，第14815-14827页，2021年。C. J. Liu、C. H. Zhu、X. Liu、M. Nie、H. Yang 和 C. X. Pei，《太赫兹频段室内环境及星间链路通信中的多载波复用连续变量量子密钥分发》，IEEE Photonics Journal，第13卷，第4期，2021年。[66] [67] R. H. Shi、J. J. Shi、Y. Guo、X. Q. Peng 和 M. H. Lee，《基于三重态量子隐形传态的量子 MIMO 通信方案》，International Journal of Theoretical Physics，第50卷，第8期，第2334-2346页，2011年。[68] N. K. Kundu、S. P. Dash、M. R. McKay 和 R. K. Mallik，《MIMO 太赫兹量子密钥分发》，IEEE Communications Letters，第25卷，第10期，第3345-3349页，2021年。[69] R. Jantti、R. Di Candia、R. F. Duan 和 K. Ruttik，《多天线量子反向散射通信》，载于第36届 IEEE 全球通信大会（GLOBECOM），新加坡，新加坡，2017年12月04日至08日，载于 IEEE Globecom Workshops，2017 年。[70] H. Deng 和 A. Sayeed，《利用稀疏波束空间特征进行毫米波 MIMO 信道建模和用户定位》，载于 IEEE 第15届无线通信信号处理进展国际研讨会（SPAWC），多伦多，加拿大，2014年6月22日至25日，载于 IEEE International Workshop on Signal Processing Advances in Wireless Communications，2014年，第130-134页。[71] S. A. Busari、K. M. S. Huq、S. Mumtaz 和 J. Rodriguez，《面向5G及以后无线通信的太赫兹大规模 MIMO》，载于 IEEE 国际通信大会（IEEE ICC），上海，中华人民共和国，2019年5月20日至24日，载于 IEEE International Conference on Communications，2019年。[72] B. Kraus、N. Gisin 和 R. Renner，《使用单向经典通信的量子密钥分发协议的秘密密钥率上下界》，Physical Review Letters，第95卷，第8期，080501页，2005年。[73] R. Renner 和 J. I. Cirac，《无限维量子系统的 de Finetti 表示定理及其在量子密码学中的应用》，Physical Review Letters，第102卷，第11期，110504页，2009年。[74] F. Grosshans、G. Van Assche、J. Wenger、R. Brouri、N. J. Cerf 和 P. Grangier，《使用高斯调制相干态的量子密钥分发》，Nature，第421卷，第6920期，第238-241页，2003年。C. Weedbrook 等，《高斯量子信息》，Reviews of Modern Physics，第84卷，第2期，第621-669页，2012年。[75] C. Weedbrook、S. Pirandola、S. Lloyd 和 T. C. Ralph，《逼近经典极限的量子密码学》，Physical Review Letters，第105卷，第11期，2010年。[76] J. Y. Sun、F. J. Hu 和 S. Lucyszyn，《理想条件下0.1至100太赫兹范围内的大气衰减预测》，IEEE Access，第4卷，第9377-9399页，2016年。[77] Y. H. Yang、A. Shutler 和 D. Grischkowsky，《0.2至2太赫兹范围内大气透射的测量》，Optics Express，第19卷，第9期，第8830-8838页，2011年。[78]

附录A

A. 信道模型的计算

Alice 与 Bob 之间的信道矩阵可建模为式（4）

$$\boldsymbol{H} = \sum_{l=1}^{L} \sqrt{\gamma_l} e^{j2\pi f_c \tau_l} \psi_{N_r}(\phi_{r,LOS}) \psi_{N_t}^{\dagger}(\phi_{t,LOS})$$

其中，$\boldsymbol{H} \in \mathbb{C}^{N_r \times N_t}$，$L$ is the total number of the 多径分量，τ_l 为第 l 条多径的传播时延。视距路径（L=1）的路径损耗 γ_l 由公式（5）给出

$$\gamma_{l=1} = G_t G_r \left(\frac{\lambda}{4\pi d}\right)^2 10^{-\frac{\delta d}{10}}$$

其中，d 为 Alice 与 Bob 之间的 distance between Alice，δ 为大气损耗。$\phi_{r,\,LOS}$ 和 $\phi_{t,\,LOS}$ 分别为 Bob 观测到的到达角和来自 Alice 的出发角。$\psi_K(\theta)$ 表示包含 K 根天线的均匀线性阵列的阵列响应向量[68]：

$$\psi_K(\theta) = \frac{1}{\sqrt{K}}\left[1, e^{j2\pi\frac{d_a}{\lambda}sin\theta}, \ldots, e^{j2\pi\frac{d_a}{\lambda}(K-1)sin\theta}\right]^T \quad (17)$$

载波信号的和 d_a denote ing 和波长。本工作中我们假设 $d_a = \frac{\lambda}{2}$。该信道模型可用参考文献 [68] 提出的 a4 奇异值分解（SVD）方案描述：

$$\boldsymbol{H} = \boldsymbol{U}\boldsymbol{\Sigma}\boldsymbol{V}^{\dagger} \quad (18)$$

这里，$\boldsymbol{U} \in \mathbb{C}^{N_r \times N_r}$ an $\boldsymbol{V} \in \mathbb{C}^{N_t \times N_t}$ 是酉矩阵，s 表示 K 个移相器 matrice [69], ，且 $\boldsymbol{\Sigma}$ 给定为

$$\boldsymbol{\Sigma} = \begin{bmatrix} diag\{\sqrt{\eta_1}, \ldots, \sqrt{\eta_r}\} & \boldsymbol{0}_{r\times(N_t-r)} \\ \boldsymbol{0}_{(N_r-r)\times r} & \boldsymbol{0}_{(N_r-r)\times(N_t-r)} \end{bmatrix} \quad (19)$$

其中 $\boldsymbol{H}$ is the rank of、 and $\sqrt{\eta_1}$ r 是 $\boldsymbol{H}$ e the 的非零奇异值，由系统中分束器的透射率 [69] 产生。

如图 1(b) 所示，MIMO系统的整体模型可表示为 [68, 69]

$$\hat{\boldsymbol{a}}_B = \boldsymbol{U}^{\dagger}\boldsymbol{H}\boldsymbol{V}\hat{\boldsymbol{a}}_A + \boldsymbol{U}^{\dagger}\boldsymbol{U}\boldsymbol{S}\hat{\boldsymbol{a}}_E \quad (20)$$

其中 $\hat{\boldsymbol{a}}_B = [\hat{a}_{B,1}, \ldots, \hat{a}_{B,\,N_r}]$ d 模式，^{T} is the receive of Bob $\hat{\boldsymbol{a}}_A = [\hat{a}_{A,1}, \quad \hat{a}_{E,1}, \quad \hat{a}_{E\,N_t}]^T$ $\hat{\boldsymbol{a}}_E = \ldots, \ , \ _{N_t}]^T$ 是 Alice 的发送模式，...，，是 Eve 注入的高斯模式。

$$\boldsymbol{S} = diag\{\sqrt{1-\eta_1}, \ldots, \sqrt{1-\eta_r}, \boldsymbol{1}_{(M-r)\times 1}\} \quad (21)$$

是一个 di $\boldsymbol{V}$ = min(N_t, N_r) t $\boldsymbol{U}^{\dagger}\boldsymbol{U} = \boldsymbol{I}_{N_r}$ ，We ge $\boldsymbol{V}^{\dagger}\boldsymbol{V} = \boldsymbol{I}_{N_t}$ as $\boldsymbol{U}$ 和 $\boldsymbol{V}$ 是酉矩阵。考虑式 (18) $\boldsymbol{H} = \boldsymbol{U}\boldsymbol{\Sigma}\boldsymbol{V}^{\dagger}$、对角矩阵 $\boldsymbol{\Sigma}$ 和 $\boldsymbol{S}$，式 (20) 可化为 $\hat{\boldsymbol{a}}_B = \boldsymbol{U}^{\dagger}\boldsymbol{U}\boldsymbol{\Sigma}\boldsymbol{V}^{\dagger}\boldsymbol{V}\hat{\boldsymbol{a}}_A + \boldsymbol{U}^{\dagger}\boldsymbol{U}\boldsymbol{S}\hat{\boldsymbol{a}}_E = \boldsymbol{\Sigma}\hat{\boldsymbol{a}}_A + \boldsymbol{S}\hat{\boldsymbol{a}}_E$。因此，Alice 与 Bob 之间的有效信道可分解为 r 个并行 SISO 信道。

Bob 随机选择输入的正交分量并进行零差测量。于是，对于第 i 个并行信道，Bob 接收的正交分量 $\hat{X}_{B,\,i}$ 与 Alice 发送的正交分量 $\hat{X}_{A,\,i}$ 之间的输入—输出关系可由一个通用量子信道表示为 [68]

$$\hat{X}_{B,i} = \sqrt{T_i}\hat{X}_{A,i} + \sqrt{1-T_i}\hat{X}_{E,i}, \qquad i = 1,2,\ldots,r \quad (22)$$

with $X_{T,\,i}$ and 分别表示透射率和 Eve 的过量噪声正交分量。Eve 的辅助模式可表示为：

$$\hat{X}_{E',i} = -\sqrt{1-T_i}\hat{X}_{A,i} + \sqrt{T_i}\hat{X}_{E,i}, \qquad i = 1,2,\ldots,r \quad (23)$$

B. 密钥率的计算

密钥率 $R^{\blacktriangleleft} = I(a{:}\,b) - I(E{:}\,b)$ 由互信息定义。假设模拟时采用高斯统计量，则 Alice 与 Bob 之间的互信息为

$$\mathrm{I(a{:}\,b)} = \frac{1}{2}log_2[1 + \frac{TV_s}{\Lambda(V_0, W)}]$$

$$\Lambda(\mathrm{x,y}) = \mathrm{Tx} + (1-\mathrm{T})\mathrm{y}$$

而 Eve 所获取的信息受到 Holevo信息 I(E: b) 的限制，其定义为

$$\mathrm{I(E:b)} = H_E - H_{E|b} \tag{24}$$

$$H_E = h(v_1) + h(v_2) \tag{25}$$

$$H_{E|b} = h(v_3) + h(v_4) \tag{26}$$

其中，H_E 和$H_{E|b}$ 分别是 Eve 的总状态和条件状态的冯·诺依曼熵 [68, 75]。冯·诺依曼熵取决于辛特征值，其表达式为 [68]

$$v_1 = \Lambda(\mathrm{W}, V_a), v_2 = \mathrm{W}, \tag{27}$$

$$v_3, v_4 = \sqrt{\frac{1}{2}(\Delta \pm \sqrt{\Delta^2 - 4\Upsilon})}, \tag{28}$$

and

$$\Delta = \frac{V_a W \Lambda(W, V_a) + W\Lambda(WV_a, 1)}{\Lambda(V_a, W)} \tag{29}$$

$$\Upsilon = \frac{V_a W^2 \Lambda(W, V_a)\Lambda(WV_a, 1)}{\Lambda^2(V_a, W)} \tag{30}$$

函数 h x ( ) is defined as

$$\mathrm{h(x)} = \frac{x+1}{2} log_2\left(\frac{x+1}{2}\right) - \frac{x-1}{2} log_2\left(\frac{x-1}{2}\right) \tag{31}$$