MIMO Terahertz Quantum Key Distribution

Neel Kanth Kundu* , Soumya P. Dash†, Matthew R. McKay*, and Ranjan K. Mallik+

*Hong Kong University of Science and Technology, †Indian Institute of Technology Bhubaneswar, +Indian Institute of Technology Delhi

1. Abstract

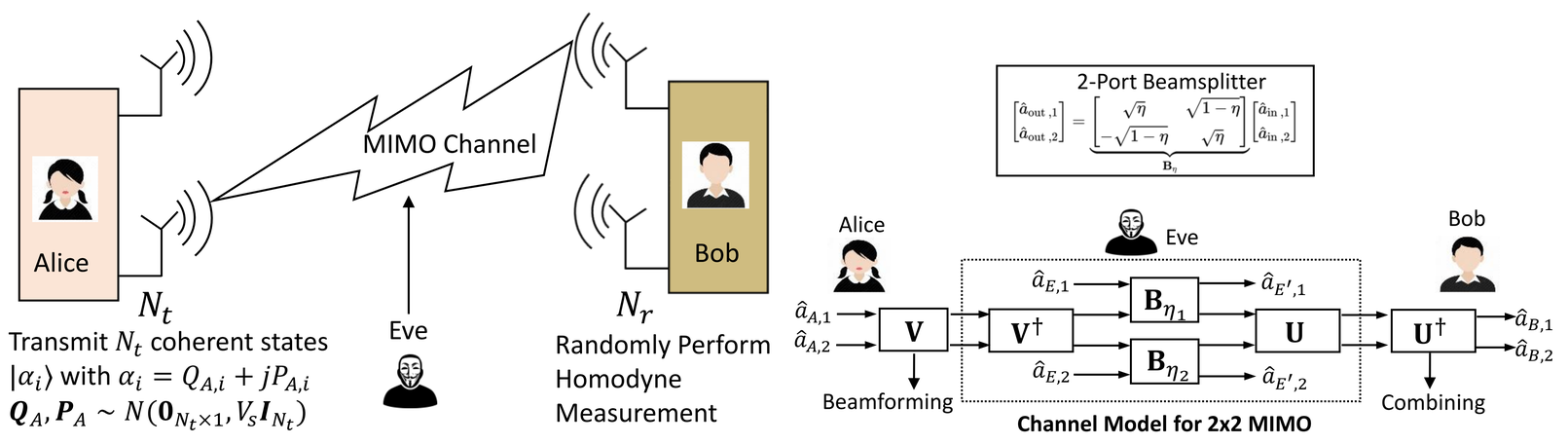
A multiple-input multiple-output (MIMO) continuous variable quantum key distribution (CVQKD) scheme is proposed for improving the secret key rates and increasing the maximum transmission distance for terahertz (THz) CVQKD applications. Further, a transmit beamforming and receive combining scheme is proposed that converts the rank-r MIMO channel between Alice and Bob into r parallel lossy quantum channels whose transmittances depend on the non-zero singular values of the MIMO channel. The MIMO transmission scheme provides a multiplexing gain of r, along with a beamforming and array gain equal to the product of the number of transmit and receive antennas. Our simulation results show that multiple antennas are necessary to overcome the high free-space path loss at THz frequencies. Thus THz MIMO CVQKD can be used for beyond 5G ultra-secure networks.

2. Introduction

With over 4.7B internet users worldwide, the security and privacy of users using banking, email and social media is very important. The security of the current cryptography algorithms using RSA and AES can be broken by a near-term Quantum computer by using Shor's and Grover's algorithm. Quantum Key Distribution (QKD) provides unconditional security which is guaranteed by the laws of quantum physics. Optical wireless links are good for point-to-point QKD links which does not support mobility. Microwave frequency has higher preparation thermal noise, hence it is not suitable for mobile CVQKD applications. Terahertz frequency range which is a candidate spectrum for 6G and has a reasonable preparation thermal noise can potentially be used for mobile CVQKD applications.

3. MIMO QKD

The schematic of the MIMO CVQKD scheme is shown in the following figure.



4. System Model

The MIMO terahertz channel model between Alice and Bob is given by [1]

$$\mathbf{H} = \sum_{l=1}^{L} \sqrt{\gamma_l} e^{j2\pi f_c \tau_l} \boldsymbol{\psi}_R\left(\phi_l^r\right) \boldsymbol{\psi}_T^\dagger\left(\phi_l^t\right) , \qquad (1)$$

Let $\mathbf{H} = \mathbf{U}\boldsymbol{\Sigma}\mathbf{V}^\dagger$ be the SVD of $\mathbf{H}$, then the input-output (I/O) relation between Alice and Bob is (without beamforming) [1]:

$$\hat{\boldsymbol{a}}_B = \mathbf{U}\boldsymbol{\Sigma}\mathbf{V}^\dagger\hat{\boldsymbol{a}}_A + \mathbf{U}\mathbf{S}\hat{\boldsymbol{a}}_E\,, \qquad (2)$$

Alice uses $\mathbf{V}$ for beamforming and Bob uses $\mathbf{U}^\dagger$ for coherent combining, then the I/O is given by

$$\hat{\boldsymbol{a}}_B = \mathbf{U}^\dagger\mathbf{H}\mathbf{V}\hat{\boldsymbol{a}}_A + \mathbf{U}^\dagger\mathbf{U}\mathbf{S}\hat{\boldsymbol{a}}_E\,. \qquad (3)$$

Let r be the rank of $\mathbf{H}$, then we have r parallel SISO channels between Alice and Bob:

$$\hat{a}_{B,i} = \sqrt{T_i}\hat{a}_{A,i} + \sqrt{1-T_i}\hat{a}_{E,i}\ ,\ i = 1, 2, \ldots, r, \qquad (4)$$

where $\sqrt{T_i}$ is the i-th non-zero singular value of $\mathbf{H}$. Bob randomly chooses one of the quadratures and performs homodyne measurement giving the I/O ($i = 1, 2, \ldots, r$):

$$\hat{X}_{B,i} = \sqrt{T_i}\hat{X}_{A,i} + \sqrt{1-T_i}\hat{X}_{E,i} \qquad (5)$$

and the input-output of Eve's ancilla mode is

$$\hat{X}_{E',i} = -\sqrt{1-T_i}\hat{X}_{A,i} + \sqrt{T_i}\hat{X}_{E,i} \qquad (6)$$

5. Secret Key Rate

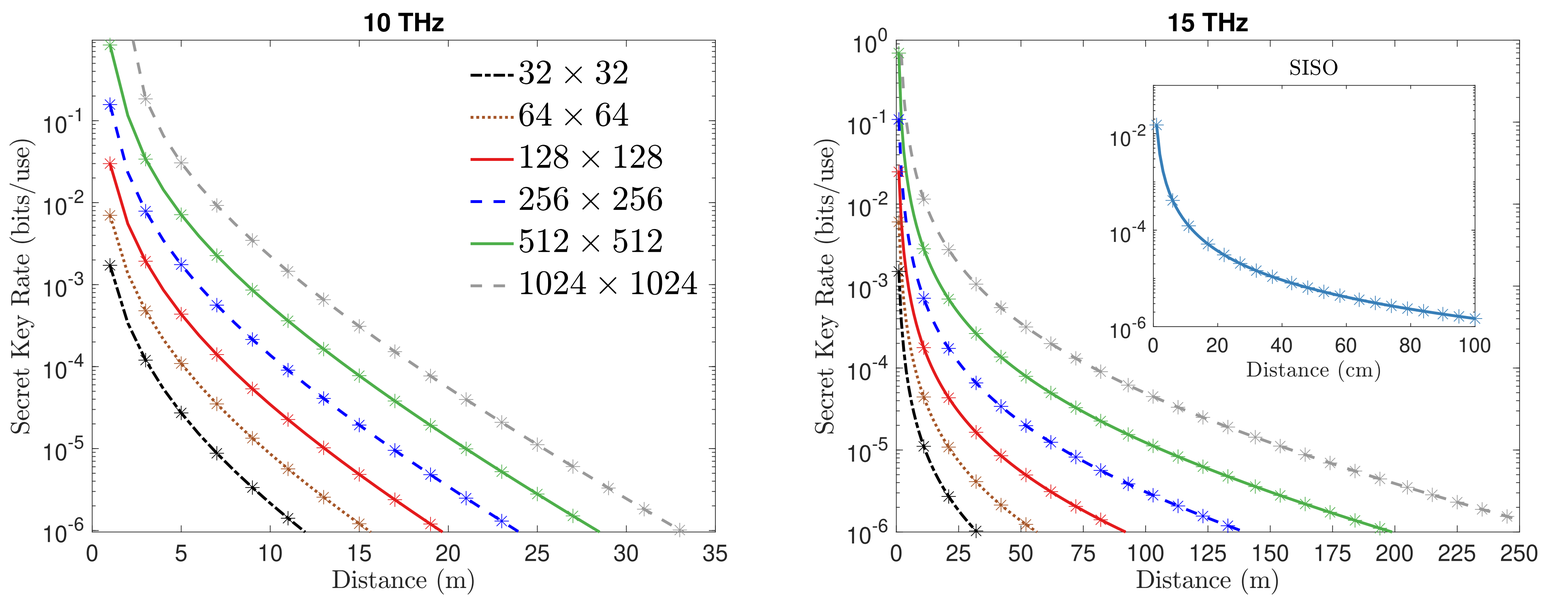
In the large modulation limit, the secret key rate is given by (V_s is Alice's transmitted signal variance, V_0 is preparation thermal noise, W is the variance of the noise injected by Eve, $V_a = V_s + V_0$ and $\Lambda_i(x, y) \triangleq T_i x + (1 - T_i)$)

$$R^{\blacktriangleleft}_{\text{MIMO}} \approx \sum_{i=1}^{r}\left(\frac{1}{2}\log_2\left[1 + \frac{T_i V_s}{\Lambda_i(V_0, W)}\right] - h\left(\Lambda_i\left(W, V_a\right)\right) - h(W) + h\left(\sqrt{\frac{V_a W \Lambda_i(W, V_a)}{\Lambda_i(V_a, W)}}\right) + h\left(\sqrt{\frac{W\Lambda_i(WV_a, 1)}{\Lambda_i(V_a, W)}}\right)\right)$$

MIMO scheme provides a multiplexing gain of r. Taylor series expansion of secret key rate is given by: $R^{\blacktriangleleft}_{\text{MIMO}} \approx 0.72\text{tr}\left(\mathbf{H}^\dagger\mathbf{H}\right)\left[\frac{V_s}{W} - \ln\left(\frac{V_a+1}{V_a-1}\right)\left(\frac{V_a^2 - W^2}{2W} - V_a\right)\right] - rh(W)$

Since, $\text{tr}\left(\mathbf{H}^\dagger\mathbf{H}\right) \propto N_r N_t$, thus MIMO scheme provides a beamforming gain of $N_r N_t$ as compared to the SISO scheme.

6. Simulation Result



It can be observed that the transmission distance is in centimeters with single antenna (SISO) system while it can be in meters for MIMO scheme. The vertical shift in the secret key rate for a given distance is due the beamforming gain from the MIMO transmission scheme.

7. Conclusions

1. We have proposed a MIMO THz CVQKD for beyond 5G wireless networks
2. SVD based beamforming and combining converts the rank r-MIMO channel into r parallel SISO channels providing a multiplexing gain of r.
3. The beamforming gain from MIMO increases the effective channel transmittance which in turn increases the secret key rate and the maximum transmission distance of MIMO scheme as compared to SISO scheme.
4. MIMO scheme is necessary to overcome the high free-space path loss and atmospheric absorption loss and achieve positive secret key rate for indoor and outdoor applications.
5. Future extensions of this work should incorporate the finite size effects and the channel estimation errors in the secret key rate analysis.

8. References

[1] N. K. Kundu, S. P. Dash, M. R. McKay, and R. K. Mallik. MIMO terahertz quantum key distribution. *arXiv preprint arXiv:2105.03642*, 2021.