Received: 23 December 2023 | Revised: 4 January 2024 | Accepted: 5 January 2024

IET Quantum Communication

DOI: 10.1049/qtc2.12085

REVIEW

Wireless quantum key distribution at terahertz frequencies: Opportunities and challenges

Neel Kanth Kundu[1,2] | Matthew R. McKay[2] | Ranjan K. Mallik[3]

[1]Centre for Applied Research in Electronics (CARE), Indian Institute of Technology Delhi, New Delhi, India

[2]Department of Electrical and Electronic Engineering, University of Melbourne, Melbourne, Victoria, Australia

[3]Department of Electrical Engineering, Indian Institute of Technology Delhi, New Delhi, India

Correspondence

Neel Kanth Kundu, CARE, Indian Institute of Technology Delhi, Room 219, Block-III, Hauz Khas, New Delhi 110016, India.
Email: neelkanth@iitd.ac.in

Funding information

Indian Institute of Technology Delhi, Grant/Award Number: New Faculty Seed Grant; Science and Engineering Research Board, Grant/Award Number: J. C. Bose Fellowship; Australian Research Council, Grant/Award Number: Future Fellowship (project number FT200100928); Department of Science and Technology, Ministry of Science and Technology, India, Grant/Award Number: INSPIRE Faculty Fellowship (Reg. No.: IFA22-ENG 34; Australian Government

Abstract

Quantum key distribution (QKD) is one of the major applications of quantum information technology. It can provide ultra-secure key distribution with security guaranteed by the laws of quantum physics. Quantum key distribution is necessary to protect data transmission from quantum computing attacks in future communication networks. The laws of quantum mechanics dictate that as opposed to microwave frequencies, quantum coherence is preserved at room temperatures for terahertz (THz) frequencies. This makes the THz band a promising solution for room-temperature QKD implementation in future wireless communication networks. The authors present the principles of continuous variable QKD (CV-QKD) systems and review the latest developments in the design and analysis of CV-QKD systems operating at microwave and THz frequencies. The authors also discuss how multiple-input multiple-output transmission can be incorporated into the quantum communications framework to improve the secret key rates and increase the coverage distances of the THz CV-QKD system. Furthermore, major hardware challenges that must be surmounted to practically realise THz CV-QKD systems are highlighted.

KEYWORDS

quantum communication, quantum cryptography, quantum information, telecommunication channels, telecommunication security

1 | INTRODUCTION

In recent years, wireless communication technology has had widespread proliferation, with diverse applications including the Internet of Things [1, 2], mobile broadband [3], intelligent transportation, healthcare [4, 5], and financial services [6]. Ensuring the highest level of data security and privacy is a crucial requirement for future wireless systems. Traditional public key encryption algorithms such as rivest-shamir-adleman and classical key distribution algorithms such as Diffie-Hellman are only computationally secure [7–9]. The security of these algorithms is guaranteed under the classical computing framework, where the problems of large prime factorisation and discrete logarithms have exponential computational complexity. However, there exists a quantum algorithm known as Shor's factoring algorithm that can efficiently solve the prime factorisation and discrete logarithm problems in polynomial time on a quantum computer [10]. With advances in quantum computing hardware, it is necessary to develop quantum-safe encryption algorithms to safeguard the security of sensitive data from quantum attacks [11, 12].

While the security of current encryption algorithms may be compromised by quantum computing, unconditional information-theoretic security can be achieved even in the presence of a powerful quantum computer by using another quantum technology known as quantum key distribution (QKD) [13]. Quantum key distribution provides a means to counter quantum attacks using quantum communication technology. Quantum key distribution is a key distribution

protocol that distributes a quantum secure key between two users whose security is guaranteed by the laws of quantum mechanics (no-cloning theorem and quantum uncertainty principle) [13]. The quantum secure key obtained from the QKD protocol can be used for symmetric key encryption by the higher layers of the protocol stack as well as at the physical layer for one-time-pad (OTP) based encryption.

In a QKD protocol, the sender (Alice) encodes the key within the quantum states of electromagnetic (EM) waves and transmits them to the receiver (Bob) via an insecure quantum channel. The receiver performs quantum measurements on the received quantum state to extract the key information. After the quantum communication step, the trusted parties carry out a post-processing step over a classical authenticated channel (CAC) to detect the presence of an eavesdropper and extract the final secret key.

There are two categories of QKD, which are determined by the specific quantum states employed for encoding the key: discrete variable QKD (DV-QKD), which employs the polarisation state of single photons, and continuous variable QKD (CV-QKD), which uses the quadratures of coherent quantum states for encoding the key information. Single-photon sources and detectors are required for DV-QKD, whereas CV-QKD can be implemented using coherent sources (lasers) and homodyne/heterodyne detectors. From a practical implementation perspective, single photon sources and detectors are difficult to realise using the current quantum hardware technology, whereas it is relatively easier to implement CV-QKD since it requires coherent sources and homodyne/heterodyne detectors. Therefore, CV-QKD stands as a promising contender for integrating QKD in next-generation communication networks.

Quantum coherence is maintained at room temperature for optical frequencies of the EM spectrum. Optical fibre-based QKD has reached significant technological maturity and may be employed for distributing quantum secure keys in core optical fibre networks. However, the implementation of QKD in wireless access networks using free-space optical communication is still a challenge. Free-space optical QKD requires accurate line-of-sight links, and its performance is deteriorated by bad weather conditions, including fog, dust, and atmospheric turbulence effects. These challenges can be overcome by using lower frequencies in the terahertz (THz) band, which requires less delicate pointing and tracking of the receiver and is immune to bad weather conditions and atmospheric turbulence. It is not possible to operate QKD at room temperature using lower frequency bands in the microwave and mmWave spectrum due to the high preparation thermal noise. Therefore, the THz band is a suitable frequency band between optical and radio frequencies at which quantum coherence is preserved and can be used for wireless QKD applications operating at room temperature [14–16].

In this paper, we present the principles of wireless CV-QKD systems operating at THz frequencies. The main contributions of this article can be summarised as follows:

- We review the basic principles of CV-QKD systems and explain the fundamental difference between classical coherent communications and CV-QKD systems.
- We provide a critical review of the latest developments in the design and analysis of microwave and THz CV-QKD systems.
- We review the recently proposed multiple-input-multiple-output (MIMO) transmission for THz CV-QKD system, which helps to overcome the high path loss at THz frequencies and achieve higher secret key rates (SKRs) and increased transmission distances.
- We discuss major hardware implementation challenges that need to be overcome for widespread deployment of THz CV-QKD in future communication systems.

The remainder of the paper is arranged as follows. Section 2 introduces the principles of CV-QKD and explains the fundamental difference between classical coherent communications and the CV-QKD system. Section 3 reviews the latest developments in microwave and THz quantum communications. Section 4 reviews the MIMO transmission scheme for improving the performance of the THz CV-QKD system. The major hardware implementation challenges of THz QKD systems are discussed in Section 5. Finally, Section 6 delivers concluding remarks and summarises the article.

2 | QUANTUM KEY DISTRIBUTION

In the following, we review the principles of the CV-QKD protocol and outline the fundamental differences between CV-QKD and classical physical layer key distribution protocols.

2.1 | Continuous variable QKD

In a general CV-QKD protocol, there are two main steps: quantum communication phase and classical post-processing phase. A schematic of the CV-QKD protocol summarising the main steps is shown in Figure 1. The first step is the quantum communication phase where the key information is encoded within the quadratures of quantum states, prior to transmission by Alice to Bob. Alice generates independent

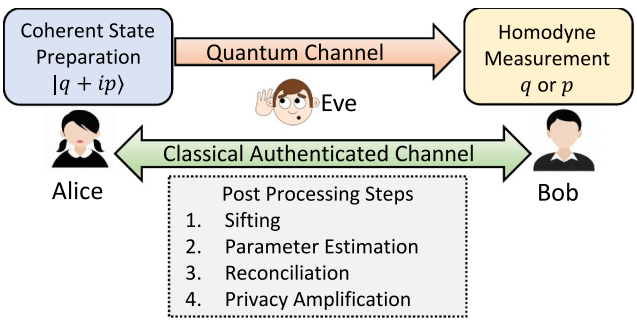


FIGURE 1 Schematic of a continuous variable QKD (CV-QKD) protocol.

bivariate real Gaussian random variables which are encoded on the q and p quadratures of the coherent quantum state; that is, Alice generates a displaced coherent state whose displacement vector depends on the bivariate real Gaussian random variables. This displaced coherent state is then transmitted to Bob over an insecure quantum channel that can be fully controlled by the eavesdropper (Eve); that is, Eve can carry out any general quantum operation on the quantum states. Bob performs either homodyne or heterodyne measurements on the received quantum state to measure either one or both quadratures, respectively. For the homodyne measurement, Bob randomly chooses to measure one of the quadratures, q or p, by flipping a fair coin or by using a quantum random number generator (to get true randomness). At the end of this step, Alice and Bob share either one or two pairs of correlated random variables depending on the type of measurement performed by Bob: homodyne (one pair) and heterodyne (two pairs). Alice and Bob repeat this quantum communication step a number of times to generate a string of correlated random variables.

In the next phase of the CV-QKD protocol, Alice and Bob carry out classical post-processing steps over a CAC to extract the final binary keys from the correlated string of (real-valued) random variables. Eve can listen to the classical messages shared over the CAC, but cannot modify these messages. Alice and Bob can verify that these messages originated from a legitimate party. The main classical post-processing steps are as follows:

1) **Sifting:** In the sifting procedure, Alice and Bob discard the irrelevant random variables. This is specifically required for the homodyne measurement scheme where Bob reveals which quadrature (q or p) was measured for each of the incoming quantum states, and Alice keeps only one of the two random variables that correspond to the measurement quadrature of Bob.
2) **Parameter Estimation:** Due to the presence of Eve and other noise sources (preparation, background, and detector noise), the sifted keys between Alice and Bob will be correlated but unidentical. Therefore, in this step, they reveal a fraction of the correlated but unidentical Gaussian keys to estimate the channel parameters including channel transmittance and noise levels.
3) **Reconciliation:** Alice and Bob then carry out a reconciliation protocol where they quantise their Gaussian keys to obtain binary keys and perform classical error correction (e.g. using low-density parity-check codes) to correct for any errors in the sifted binary keys. There can be two reconciliation protocols: direct reconciliation (DR) and reverse reconciliation (RR). In DR, Alice's Gaussian key is used as a reference for error correction such that Alice sends classical messages to Bob for error correction, whereas in RR it is vice versa. The amount of information leaked to Eve is different for DR and RR. In DR, Alice's transmitted quantum states are intercepted by Eve and Alice's classical error correction messages are also overheard by Eve which leads to higher key information being leaked to Eve. In RR, Eve can only access Bob's classical error correction messages and the quantum states received by Bob are not accessible to Eve. Therefore, the information accessible to Eve is lower for RR as compared to DR, which leads to a higher SKR for RR [13].
4) **Privacy Amplification:** After reconciliation, Alice and Bob estimate the maximum information leaked to Eve. Based on this estimate, they perform a privacy amplification in order to reduce the length of the binary key, which can substantially reduce the knowledge Eve has about the final secret key. This can be achieved by employing a random hash function [13].

2.2 | Classical key distribution versus continuous variable QKD

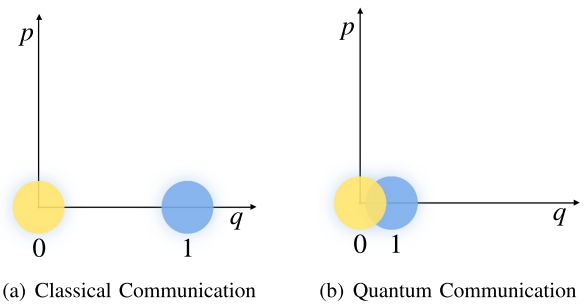
Here, we discuss the fundamental differences between classical information-theoretic key distribution protocols and CV-QKD protocols.

Classical physical layer encryption and key distribution protocols are derived from Wyner's wiretap channel model. The key shared between Alice and Bob is perfectly secure from the eavesdropper under the assumptions of classical physics only. The achievable SKR is calculated using the tools of classical information theory where the SKR is the difference between classical Shannon's mutual information of the Alice-Bob main channel and Shannon's mutual information of the Alice-Eve wiretap channel [17]. However, any communication channel is fundamentally quantum mechanical. The CV-QKD protocol guarantees perfect security under the quantum mechanical framework where Eve can perform any operation (valid under the laws of quantum mechanics) for eavesdropping. Quantum information theory tools are used to evaluate the SKR of the CV-QKD protocol. Since the key information is encoded by Alice in the quadratures of the coherent state and Bob uses homodyne/heterodyne measurement, the mutual information between Alice and Bob corresponds to classical Shannon's information. However, in order to guarantee perfect secrecy even in the presence of quantum attacks, the amount of information that is accessible to Eve is evaluated using quantum Holevo information. The achievable SKR of CV-QKD is thus given by the difference between Shannon's mutual information between Alice-Bob and the quantum Holevo information between the eavesdropper state and Alice (Bob) depending on the type of reconciliation used, that is, DR (RR). As compared to the classical information-theoretic key distribution, CV-QKD employs a conservative approach to evaluate the SKR by assuming a worst-case scenario where the eavesdropper can steal the maximum key information allowed by the laws of quantum mechanics. The eavesdropper can access the maximum key information (given by Holevo information) by performing a joint quantum measurement on a stored ancilla quantum state and the quantum state used for intercepting the main quantum communication channel between Alice and Bob.

The fundamental difference between the key distribution protocols using classical coherent communications and CV-

QKD can be intuitively understood as follows. Although, for both classical coherent communications and CV-QKD, the key information is encoded within the quadratures of the coherent states, in the quantum regime very low transmission powers of the order of quantum shot noise are used. On the other hand, in classical communications, the transmitted power is quite high such that the quantum shot noise becomes insignificant as compared to the signal power. Therefore, the eavesdropper can intercept and retransmit the signal without leaving a signature, such that Alice and Bob will not be able to detect Eve's presence. However, in the quantum regime, it is impossible to perfectly intercept the information without leaving a signature due to the fundamental quantum shot noise. This is pictorially depicted for a simple example in Figure 2. Here, in classical coherent communication, Alice uses On-Off keying to encode '0' with no signal and '1' with a high-power signal, where the q quadrature is displaced by a large quantity. In the quantum mechanical description of the EM wave, there is an uncertainty even in the absence of a signal. This is denoted by the circular region in Figure 2 which is known as the vacuum shot noise. In Figure 2a, the quantum uncertainty depicted by the circular area is insignificant as compared to the displacement, so Eve can perfectly discriminate the two states and decode the key information. In the classical case, Eve can perform an intercept and resend attack, without leaving a signature that cannot be detected by Alice and Bob during the post-processing step. However, in the quantum case, Alice uses a small displacement in the q quadrature to encode key '1' such that the uncertainty cloud of '0' and '1' overlap, as shown in Figure-2b. In this case, Eve cannot perfectly discriminate between '0' and '1' due to the inherent quantum noise. Therefore, Eve will leave a signature and make errors in the intercept and resent attack that will be detected by Alice and Bob during the post-processing step.

Furthermore, we note that the physical layer key generation scheme using the shared randomness of the wireless channel between Alice and Bob is also not perfectly secure [17]. If Eve is close to Bob, then the Alice-Bob wireless channel will be correlated to the Alice-Eve channel thereby allowing Eve to extract the key information from the correlated wireless channel. Therefore, these security loopholes can be overcome by using CV-QKD, which ensures security based on the fundamental principles of quantum physics.



(a) Classical Communication (b) Quantum Communication

FIGURE 2 Classical versus quantum communication.

3 | QUANTUM COMMUNICATIONS AT MICROWAVE AND THz FREQUENCIES

Recently, there has been an increasing interest in developing quantum communication technologies operating at microwave and terahertz frequencies [14, 18, 19]. Different from optical frequencies, THz and microwave frequencies have robust performance in bad weather conditions since they are less affected by adverse weather conditions of rain, haze, and fog [20–24]. Furthermore, microwave quantum communications are also motivated by the recent progress in superconducting quantum computing technology operating in the microwave regime. The development of microwave quantum communications and QKD will lead to the seamless integration of distributed quantum computing resources and lead to the development of local quantum networks [25].

3.1 | Microwave continuous variable QKD

The implementation of CV-QKD at lower frequencies requires the generation and detection of Gaussian quantum states at microwave and THz frequencies, which are necessary for encoding the key information in the first quantum communication phase of the CV-QKD protocol. The rest of the classical post-processing steps over the CAC remain the same as discussed in Section 2.1. As compared to optical Gaussian coherent states, the Gaussian quantum state generated at microwave and THz frequencies is a Gaussian thermal state having a higher preparation thermal noise [14]. The inherent quantum uncertainty in the quadrature measurement arising from Heisenberg's uncertainty principle is characterised by the thermal noise variance V_0. The thermal noise variance depends on the frequency (f) of operation and environmental temperature (T_e) and is given in terms of the average number of thermal photons (n) as $V_0 = 2n + 1$ shot noise unit (SNU). Here, the n is characterised using the Bose-Einstein distribution as $n = [\exp(hf/k_B T_e) - 1]^{-1}$, where h and k_B denote the Planck's constant and Boltzmann's constant, respectively. For optical frequencies, $n \approx 0$, such that $V_0 \approx 1$ SNU at room temperature. However, for lower frequency ranges $n \gg 1$, and hence $V_0 \gg 1$ SNU at room temperature, for example, in the microwave regime of $f = 5$ GHz, $n = 1250$. This is the main limiting factor in the implementation of CV-QKD at lower frequency bands.

A theoretical feasibility study of the microwave CV-QKD system was carried out by the authors of ref. [18]. In this work, the authors presented a system model for microwave CV-QKD and characterised the coupling of propagating microwave Gaussian quantum states with the environmental thermal background state. The authors proposed a squeezed state-based CV-QKD protocol where Alice uses displaced

squeezed states to encode the key information, and Bob uses homodyne detection to measure the quadrature of the incoming microwave quantum state. In order to preserve the quantum coherence at microwave frequencies, the generation and detection of microwave quantum states require cryogenic refrigerators operating at milli Kelvin (mK) temperatures [18]. This can be understood from the Bose-Einstein distribution, which characterises the average number of thermal noise photons (n) at frequency f operating at temperature T, $n = [\exp(hf/k_BT_e) - 1]^{-1}$ where h and k_B denote the Planck's constant and Boltzmann's constant, respectively. For optical frequencies $n \approx 0$ at room temperature $T = 300$ K, whereas for microwave frequency, say $f = 5$ GHz, $n = 1250$ at $T = 300$ K. Therefore, microwave quantum communications require cryogenic cooling in mK to achieve $n \approx 0$ at $f = 1$–10 GHz [26]. The authors of ref. [18] neglected the effects of free space path loss of microwave propagation and assumed that antennas of sufficient gains are used at the transmitter and receiver to compensate for up to 80 dB of free space path loss. The authors considered only the effect of atmospheric absorption losses to compare the SKR performance of microwave and optical CV-QKD protocols. The simulation results of ref. [18] reveal that microwave CV-QKD can support positive SKRs up to a distance of 200 m using both DR and RR schemes. Furthermore, the results reveal that there exists a threshold crossover distance (d_c), below which the SKR of microwave CV-QKD is higher than that of optical CV-QKD for practically available bandwidths at these frequencies. While the maximum secure distance for optical CV-QKD is severely degraded in bad weather conditions, the secure distance for microwave CV-QKD is unaffected in rain, haze, and fog conditions, which indicates the robustness of microwave CV-QKD [18]. Overall, the results of ref. [18] indicate that open-air microwave CV-QKD is practically feasible using cryogenic microwave quantum technology. Therefore, a hybrid quantum communication network can be developed in the future, where microwave CV-QKD can be used for short-distance applications, whereas optical CV-QKD can provide quantum security at longer distances.

Recently, an experimental prototype of microwave CV-QKD was demonstrated by the authors of ref. [19] where cryogenic cooling was used for the transmitter, receiver, as well as for quantum channel. The untrusted, lossy, and noisy quantum channel was experimentally realised using a cryogenic directional coupler with fixed power losses and tunable Gaussian noise. The microwave CV-QKD was implemented at 5.48 GHz using a superconducting Josephson parametric amplifier (JPA) for generating squeezed Gaussian microwave quantum states. The JPAs consist of a coplanar waveguide resonator and a direct current superconducting quantum interference device, which enables continuous frequency tuning of the JPAs. In order to encode the random Gaussian, Alice displaces the quadrature of the squeezed state by using a cryogenic directional coupler. At the receiver, the homodyne detection of the quadrature of the incoming microwave quantum state is implemented using superconducting phase-sensitive amplifiers facilitated by a secondary JPA. The experimental demonstration in ref. [19] can be viewed a simulation of a real-world microwave CV-QKD protocol where the thermal background temperature of the quantum channel can be controllably varied to study the SKR of the protocol. The analysis of ref. [19] reveals that unconditionally secure microwave CV-QKD is feasible up to a distance of 1200 m in a cryogenic environment, which corresponds to a secure distance of 80 m in open-air microwave CV-QKD under the assumptions of high gain microwave antennas which compensates for the free space path loss. This experimental demonstration is an important milestone in the development of free space microwave CV-QKD systems and quantum local area networking using superconducting quantum circuits in future communication networks [27].

Although microwave CV-QKD is a promising solution for short-distance quantum communication applications, its widespread commercial deployment is limited by the requirement of expensive cryogenic cooling equipment. Therefore, alternative solutions are required to support CV-QKD operating at room temperature that can overcome the limitations of optical CV-QKD systems.

3.2 | THz continuous variable QKD

The THz frequency range lies in between the lower microwave and higher optical frequency band. As the frequency of the EM waves increases from microwave to THz (closer to the optical band), the quantum effects become more evident. THz frequency band has the potential to offer the best of both worlds, including robust performance in adverse weather conditions (similar to microwave band) and depicting the quantum mechanical properties (similar to the optical band). Therefore, the unique quantum mechanical properties of the THz band can be harnessed for enhanced performance in communications and information processing applications. The fundamental randomness arising from the quantum shot noise at THz frequencies can be used for secure physical layer encryption [28]. Recently, researchers have started investigating the application of THz frequencies for room temperature operation of CV-QKD [14]. At room temperature ($T = 300$ K) for a frequency of $f = 30$ THz, the average number of thermal photons is $n = 8.3 \times 10^{-3}$, which is much lower than $n = 1250$ at $f = 5$ GHz. Therefore, the THz band offers a sweet spot between higher optical frequencies and lower microwave frequencies that can support CV-QKD protocol at room temperatures [14]. Furthermore, the THz band is also being considered as a potential spectrum for future classical communication networks due to the availability of huge bandwidths that can support high data rates. Thus, THz can support both high data rate classical communications and secure quantum communications in future wireless networks.

Recent studies have examined the viability and practical challenges of THz CV-QKD systems [14–16]. These initial

works have characterised the secret key rate (SKR) of a single-input-single-output (SISO) THz CV-QKD system. The authors of ref. [15] investigated the feasibility of THz CV-QKD systems operating in the frequency range of 0.1–1 THz. The SKR results of ref. [15] reveal that 0.1–1 THz frequency band can support only very short secrecy distances of the order of 2 m. The authors of ref. [15] outlined a possible implementation of the THz CV-QKD system using THz quantum sources and electro-optical amplitude/phase modulators at the transmitters. At the receiver, the quadrature of the THz quantum state is measured using a THz homodyne detector that can be realised using THz beamsplitters and plasmonic photoconductive detectors or single THz photon detectors [15].

The authors of ref. [14] studied the SKR performance in the extended THz range of 1–50 THz and characterised the asymptotic SKR for both DR and RR reconciliation schemes. However, it has to be noted that the SKR analysis in ref. [14] was carried out by considering only the effect of atmospheric absorption loss and neglecting the effect of free space path loss, which can be a limiting factor for large transmission distances. Under the assumption that the free space path loss can be completely compensated using high gain antennas, the simulation results of ref. [14] reveal that high rate CV-QKD is feasible up to a few meters using DR and up to 220 m in the RR scheme. The results reveal that below 1 THz, the main limiting factor is the high thermal noise at room temperature, while at higher frequencies, the main limiting factor is the high atmospheric absorption coefficient. The authors also outlined a possible hardware architecture for the practical realisation of the THz CV-QKD system using bi-directional THz-to-optical converters at the transmitter and receiver. Since THz sources, modulators, and detectors are technologically less mature than their optical counterparts, the authors proposed a possible implementation of the THz CV-QKD system using the existing quantum optical technology of coherent laser sources, homodyne/heterodyne detection, and coherent THz-optical conversion technology. The bidirectional THz-optical conversion scheme proposed in ref. [14] is motivated by the recent technological progress in coherent microwave-optical interfaces. At the transmitter, the THz quantum state is generated by first generating a coherent quantum state at the optical frequency band, which is then fed to an optical and THz cavity mode whose output is coupled to a THz waveguide.

The authors of ref. [16] proposed an indoor channel model SISO THz CV-QKD systems using ray tracing. Different from the initial works on THz CV-QKD [14, 15] that considered only line-of-sight channels, the channel model in ref. [16] also considered the effect of the non-line-of-sight links in the indoor environment. The simulation results in ref. [16] show that a maximum secure distance of 2 m is achievable at a frequency of 0.41 THz, which is suitable for indoor applications.

Apart from terrestrial CV-QKD, the THz band has also been studied for inter-satellite QKD in space [29]. Different from terrestrial weather conditions, the temperature in space can be significantly lower, which reduces the preparation thermal noise and leads to improved SKR performance for inter-satellite CV-QKD systems operating at THz frequencies. The THz channel is adversely affected due to absorption by water and oxygen molecules in terrestrial applications. However, this deteriorating effect is significantly reduced in space due to the negligible water and oxygen concentrations in space. Therefore, THz CV-QKD is a promising solution for inter-satellite links in space. The authors of ref. [29] analysed the SKR of inter-satellite THz CV-QKD for two different operating temperatures: 173 K, which is the typical operating temperature of satellite components, and 30 K, which can be attained by using shielding and passively cooling the satellite components. The authors assume a directed LoS THz link between the satellites similar to an optical link and model the diffraction-only spreading loss using the Gaussian beam channel model. The simulation results reveal that a maximum transmission distance of a few hundred Kms is feasible for inter-satellite THz CV-QKD links [29].

Although the preparation thermal noise V_0 is low at THz frequencies, there are other challenges that limit the achievable SKR and the maximum transmission distances at THz frequencies. These include the higher atmospheric absorption loss and free-space path loss at THz frequencies that reduce the channel transmittance. The SKR results of the prior works that considered the effect of free space path loss reveal that THz CV-QKD can support only very short distances of the order of a few meters for indoor applications [15, 16]. In order to overcome the challenge of high path loss, the authors of ref. [30] proposed a MIMO transmission scheme for the THz CV-QKD system, as reviewed in the next section.

4 | MIMO THz CONTINUOUS VARIABLE QKD

MIMO is a mature technology for classical wireless communication that has been standardised in WiFi, long term evolution, and 5G networks. However, the potential of MIMO for quantum wireless communications has not been fully investigated yet. It is not trivial to extend the classical MIMO wiretap channel model to the quantum case since in the quantum case, a single quantum operation acts on Alice's transmitted quantum states and produces the quantum states accessible to Bob and Eve. The quantum mechanical description of the MIMO channel, optimal transmission, and reception schemes with and without channel state information (CSI) are some of the open problems that need to be investigated to harness the full potential of MIMO in quantum wireless communications.

In this section, we summarise our recent works on the MIMO THz CV-QKD system and present the main ideas and findings from our prior works [30–32].

Inspired by the classical singular value decomposition (SVD)-based MIMO transmission, we proposed a potential transceiver scheme for MIMO THz CV-QKD systems in ref. [30]. The SVD-based transmission scheme decomposes the MIMO quantum channel into parallel SISO Gaussian quantum channels. Although the proposed system uses the well-known SVD-based transmit-receive beamforming from classical MIMO communications, the underlying MIMO channel

model is fundamentally different in the quantum case since the transmitted and received modes need to satisfy the quantum commutator relations. The system model and asymptotic SKR analysis of the MIMO THz CV-QKD system are discussed below.

4.1 | System model and secret key rate analysis

A schematic of a 2 × 2 MIMO THz CV-QKD system proposed in ref. [30] is shown in Figure 3. In the quantum communication framework, the EM modes are represented using the annihilation operators $\hat{a}$ that satisfy the quantum commutator relations. The annihilation operator is analogous to the complex baseband signal representation used in classical communication systems.

In the MIMO CV-QKD system, Alice encodes independent key information on two EM modes $(\hat{a}_{A,1}, \hat{a}_{A,2})$ and transmits them simultaneously using multiple transmit antennas as shown in Figure 3. The transmitted annihilation operators undergo transformations according to the MIMO beamsplitter channel model [33]. The dashed box in Figure 3 is the quantum MIMO channel, which is controlled by Eve. To obtain the utmost key information, Eve generates an entangled two-mode squeezed vacuum (TMSV) state (for each transmitted mode) and mixes one of the modes $(\hat{a}_{E,1}, \hat{a}_{E,2})$ with the transmitted mode from Alice as shown in Figure 3. The other mode of the TMSV is stored in quantum memory and jointly measured with the output modes available to Eve $(\hat{a}_{E',1}, \hat{a}_{E',2})$ at the end of the quantum communication phase to steal the maximum key information. The transmitted modes from Alice are mixed with Eve's ancilla modes using a beamsplitter $\boldsymbol{B}_{\eta_1}, \boldsymbol{B}_{\eta_2}$ whose transmissivity depends on the singular values of the wireless MIMO channel (see the pink box in Figure 3). The 2-port beamsplitter matrix, shown at the top of Figure 3, performs a unitary operation on the two input modes to produce the output modes such that the quantum commutator relations are maintained at the output modes. In order to decompose the MIMO channel into parallel SISO channels, Alice performs an SVD-based pre-processing on the transmitted modes using the unitary matrix $\boldsymbol{V}$ (corresponding to the right singular vectors of the MIMO channel), and Bob performs post-processing on the received modes using the unitary matrix $\boldsymbol{U}^{\dagger}$ (left singular vectors of the MIMO channel) as shown in Figure 3. To this end, we note that the 2 × 2 MIMO CV-QKD model shown in Figure 3 can be generalised to any $N_r \times N_t$ MIMO configuration since any unitary matrix can be represented as a mesh of connected two-port beamsplitters [30].

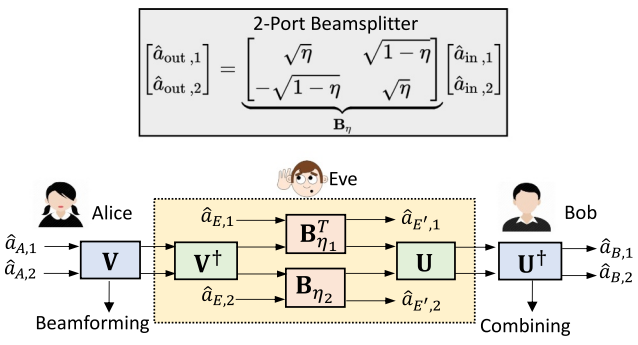
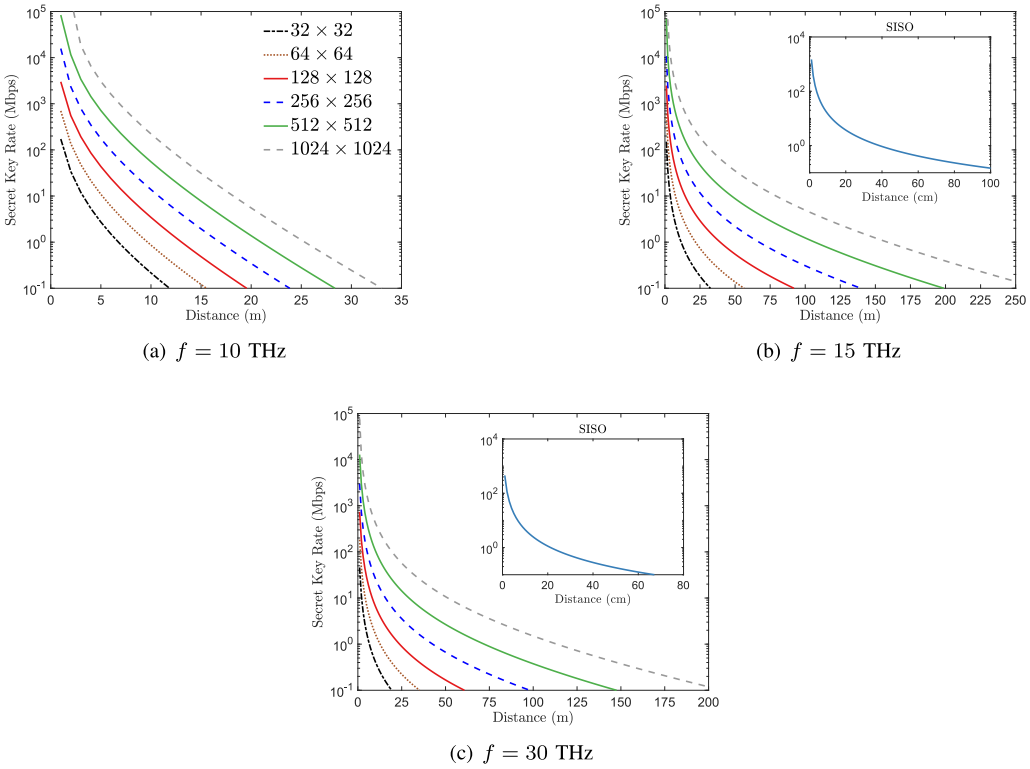


FIGURE 3 Schematic of a 2 × 2 MIMO THz continuous variable QKD (CV-QKD) system. MIMO, multiple-input multiple-output.

This transmit-receive beamforming approach, based on the SVD, provides a spatial multiplexing gain equal to the MIMO channel rank, which allows Alice and Bob to access multiple parallel SISO Gaussian channels for distributing the raw keys. For each MIMO channel use, Alice and Bob share multiple correlated random variables, that enables a higher SKR to be obtained compared with a SISO channel. The effective SKR of the MIMO CV-QKD system is equal to the sum of the SKRs of the individual SISO Gaussian quantum channels whose transmissivities are equal to the square of the singular values of the MIMO wireless channel. The asymptotic SKR of the ith parallel SISO channel corresponds to the difference between classical Shannon's mutual information of the ith pair of random variables between Alice and Bob, and the quantum Holevo information between Eve's ancilla state and Bob's measurement outcome (for the RR scheme). The asymptotic SKR of the MIMO CV-QKD system is presented in [ref. 30, Eq. (20)-(21)] and reveals that coherent transmission and reception provide a multiplexing gain equal to the rank of the MIMO channel and a beamforming or power gain proportional to the product of the number of antennas at Alice and Bob.

The SKR analysis in our prior work [30] reveals that there exists a trade-off in the achievable SKR as the carrier frequency is increased. There are two opposing factors that affect the SKR: the preparation thermal noise is reduced at higher THz frequencies (which improves the SKR), whereas the channel transmittance is reduced at higher frequencies (which degrades the SKR). Therefore, the carrier frequency needs to be carefully chosen such that positive SKRs are achievable at room temperatures. The approximate SKR analysis presented in our prior work provides a condition that needs to be satisfied in order to achieve positive SKR [30, Eq. (21)]. The condition is given by $\zeta > \alpha$ where ζ, α are given by [30, Eq. (22),(23)], respectively. The parameter ζ depends on V_0 (which in turn depends on the carrier frequency f and environment temperature T_e) and the parameter α depends on the channel transmittance and the noise introduced by Eve [30]. The numerical results in ref. [30] reveal that the condition $\zeta > \alpha$ is satisfied at the room temperature ($T_e \approx 300$ K) for the frequency range of 10–30 THz. Therefore, the 10–30 THz frequency spectrum is suitable for room temperature operation of CV-QKD systems. To this end, we note that recent work has also studied the MIMO transmission scheme for mmWave CV-QKD system; however, the implementation of CV-QKD at lower mmWave frequencies requires cryogenic cooling to a temperature of $T = 4$ K [34].

Figure 4 plots SKR (in Mbps) against transmission distance for MIMO CV-QKD schemes at three different carrier frequencies and assuming a bandwidth of 100 GHz. For comparison, the SKR plots of the baseline SISO CV-QKD system are also shown in Figure 4 for $f = 15$, 30 THz. The simulation



(a) $f = 10$ THz (b) $f = 15$ THz

(c) $f = 30$ THz

FIGURE 4 The plots show secret key rate (SKR) (in Mbps) versus transmission distance for different MIMO configurations ($N_r \times N_t$) at three different carrier frequencies and assuming a bandwidth of 100 GHz [30]. For comparison, the SKR plots of the baseline SISO continuous variable QKD (CV-QKD) system are also shown. MIMO, multiple-input multiple-output; SISO, single-input single-output.

parameters are detailed in our prior work [30]. It can be observed that the SKR performance can be significantly improved by using the MIMO CV-QKD system as compared to the baseline SISO system (note that transmission distances are in metres for MIMO and in centimetres for the SISO configuration). For a given transmission distance the vertical shift in the SKRs is due to the beamforming and power gain arising from the increasing number of transmit and receive antennas. Furthermore, the results reveal that the best SKR performance is obtained at $f = 15$ THz since the atmospheric absorption coefficient is significantly lower at this frequency. To this end, we note that classical THz communications consider frequencies in the band 0.1–10 THz for high data rate applications, however for THz CV-QKD higher frequencies in the 10–30 THz band are required to support positive SKRs at room temperature.

The plots in Figure 4b reveal that an SKR of 1 Mbps is achievable for practical transmission distances up to a few hundred metres that are suitable for both indoor and outdoor applications. Therefore, the MIMO THz CV-QKD can support OTP-based physical layer encryption with a data rate of 1 Mbps. In order to support secure data transmission with higher data rates, the secret keys need to be reused with a slight compromise in security level. For example, for the transport layer encryption algorithm, the keys can be refreshed every 3 Tb of data in order to achieve extremely low attack success probability ($\approx 2^{-60}$) [35]. Therefore, the quantum secure keys obtained from the MIMO THz CV-QKD can be used for higher layer encryption algorithms in high data rate applications with extremely low attack success probability.

4.2 | Channel estimation

Estimation of the quantum communication channel between Alice and Bob is an important step of the CV-QKD protocol, as shown in Figure 1. In the SISO CV-QKD protocol, channel estimation is carried out in the post-processing phase, where Alice and Bob reveal a fraction of their encoded keys and quadrature measurements, respectively, over the CAC [36, 37]. This is similar to the pilot-assisted channel estimation protocols used in classical communication systems [31, 38–40].

We note that different from the conventional SISO CV-QKD protocol that performs channel estimation after the quantum communication phase, in MIMO CV-QKD, channel estimation is required prior to the quantum communication phase for realising the SVD-based beamforming that decomposes the MIMO channel into parallel SISO channels as discussed in Section 4.1. The MIMO channel can be estimated at Bob prior to the quantum communication phase by transmitting known pilot symbols from Alice [31]. The estimated CSI can then be fed back to Alice using the CAC. A schematic of the pilot-assisted channel estimation protocol for the MIMO THz CV-QKD system is shown in Figure 5. Alice and Bob use the estimated CSI for implementing the SVD-based transmit-receive beamforming during the quantum communication

phase. Due to the finite pilot duration and limited transmit power, the estimated CSI has some errors. Due to imperfect CSI at Alice and Bob, the SVD-based transmit-receive beamforming is not able to completely decompose the MIMO wireless channel into noise-free parallel SISO channels. Therefore, the quadrature measured by Bob will have additional noise terms as a consequence of the channel estimation errors. This limits the practically achievable SKR due to the additional noise terms. Our prior work analysed the practically achievable SKR by accounting for the effects of pilot overhead, channel estimation errors, detector noise, and imperfect reconciliation [31]. The simulation results in ref. [31] reveal that the practically achievable SKRs are significantly degraded as compared to asymptotic SKRs, particularly at large transmission distances. The reason is that at large transmission distances, the channel estimation error increases due to lower channel transmittance. Therefore, the combined effects of increased channel estimation errors and reduced channel transmittance lead to a reduction in the practically achievable SKR at larger distances. This can be overcome by transmitting high-power pilot signals to more distant users.

4.3 | Restricted eavesdropping scenario

The MIMO THz CV-QKD system shown in Figure 3 operates under a scenario of unrestricted eavesdropping, wherein Eve possesses complete control over the environment. This enables Eve to access all the signal photons that are lost when Alice transmits to Bob, which is a pessimistic assumption used to prove the unconditional security of CV-QKD theoretically. However, in a realistic scenario, Eve is located in the wireless environment and may have access to just a portion of the signal photons that are lost in the environment [41]. The authors of ref. [41] analysed the achievable SKR of a SISO CV-QKD system in a practical scenario of restricted eavesdropping by incorporating the effect of the lossy quantum wiretap channel between Eve and the main Alice-Bob quantum channel. The restricted eavesdropping model developed in ref. [41] is a quantum analog of the classical Wyner's wiretap channel mode [42]. The restricted eavesdropping model of ref. [41] was further extended to the MIMO THz CV-QKD system in ref. [32].

A schematic of restricted eavesdropping for a 2 × 2 MIMO CV-QKD system is shown in Figure 6. Different from Figure 2 (unrestricted eavesdropping scenario), in Figure 6, the ancilla modes $(\hat{a}_{E',1}, \hat{a}_{E',2})$ are not directly available to Eve, and they undergo an additional loss on a beamsplitter $\boldsymbol{B}_\kappa$ with transmissivity κ and environment vacuum modes $(\hat{a}_{v,1}, \hat{a}_{v,2})$ such that the new output modes $(\hat{a}_{E'',1}, \hat{a}_{E'',2})$ are now available to Eve for implementing the quantum attack. The other output modes $(\hat{a}_{v',1}, \hat{a}_{v',2})$ from the beamsplitters with transmissivity κ are lost in the environment and not accessible to Eve. The quantum wiretap channel transmittance between Alice and Eve is represented by parameter κ. Note that for $\kappa = 1$, the model with restricted eavesdropping in Figure 6 collapses to the unrestricted eavesdropping model of Figure 3. The results in our prior work [32] reveal that the achievable SKR significantly improves by orders of magnitude under practical restricted eavesdropping scenarios. The reason is that the accessible information to Eve is significantly reduced in the restricted eavesdropping scenario with $\kappa < 1$. Furthermore, we also compared the SKR performance of the squeezed state-based and coherent state-based THz CV-QKD system under different eavesdropping scenarios. The results in our prior work [32] revealed that the squeezed states based THz CV-QKD protocol achieved a higher SKR for the unrestricted eavesdropping scenario ($\kappa = 1$); however, in the restricted eavesdropping scenario ($\kappa < 1$), the coherent state-based CV-QKD protocol achieved a higher SKR. Therefore, in a practical restricted eavesdropping scenario, a coherent state-based CV-QKD protocol should be used, which is also easier to realise in practice.

To this end, we note that the MIMO transmission scheme proposed in our prior works [30–32] uses the spatial division multiplexing technique to improve the SKR of the THz CV-QKD system. It is also possible to improve the SKR by using the multi-carrier multiplexing (MCM) technique, where multiple parallel CV-QKD links are established using different subcarrier frequencies. The authors of ref. [43] proposed an MCM-based THz CV-QKD system and analysed the SKR for both short-distance indoor and inter-satellite links. In the proposed MCM scheme, Alice uses a THz frequency comb synthesiser and a coupler for multiplexing the multiple Gaussian states on different sub-carriers. At the receiver, Bob

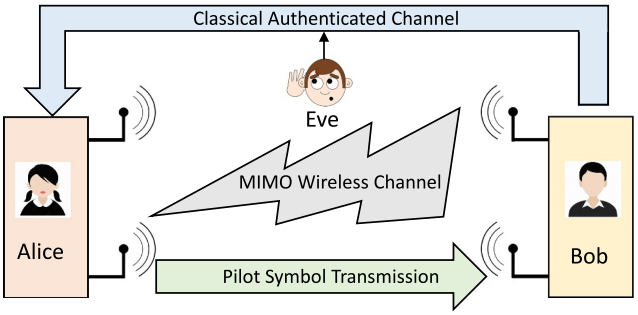


FIGURE 5 Schematic of pilot-assisted channel estimation protocol for MIMO THz continuous variable QKD (CV-QKD) system. MIMO, multiple-input multiple-output.

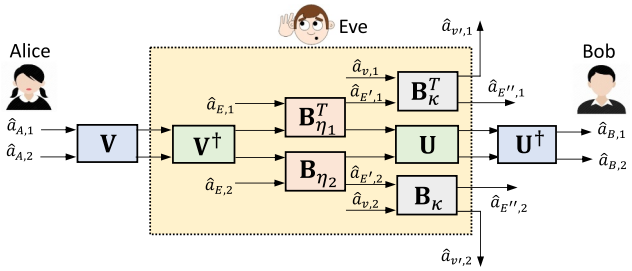


FIGURE 6 A schematic of restricted eavesdropping for a 2 × 2 MIMO continuous variable QKD (CV-QKD) system. MIMO, multiple-input multiple-output.

uses an optical discrete Fourier transform to demultiplex the different subcarriers and subsequently performs homodyne detection separately on each of the subcarriers to extract the key information from the parallel channels. The simulation results of ref. [43] reveal that for terrestrial indoor applications, a secret distance of a few metres is achievable, whereas for inter-satellite links, the secret distance can be of the order of a few hundred Kms in space. We note that the spatial domain multiplexing and demultiplexing in the MIMO THz CV-QKD systems [30–32] are realised using the SVD-based beamforming, which can be implemented using a network of beamsplitters. On the other hand, the MCM-based THz CV-QKD system proposed in ref. [43] uses a coupler for multiplexing and optical discrete Fourier transform for demultiplexing the different subcarriers.

5 | CHALLENGES IN THz CONTINUOUS VARIABLE QKD

Experimental demonstration of CV-QKD has been achieved only at optical frequencies [13] since the quantum hardware is technologically less mature at THz frequencies. Furthermore, recently an experimental prototype of microwave (5 GHz) CV-QKD has also been demonstrated using superconducting JPA, which requires cryogenic cooling. To the best of our knowledge, an experimental demonstration of THz CV-QKD operating at room temperature has not been reported in the literature yet. However, recent works have outlined the principles of physical hardware implementation that can be used for the realisation of THz CV-QKD in the future [14, 15]. Here, we describe the main hardware components required and the challenges that need to be overcome for the practical implementation of the THz CV-QKD system.

5.1 | THz sources and modulators

The main component of a THz CV-QKD system is a coherent THz source emitting signals in the 10–30 THz frequency band. In principle, there are two ways to generate THz signals. First is optical-to-THz down conversion using the principles of difference frequency generation and optical parametric process using non-linear optical crystals [44], and photo-mixing using ultra-fast photo-diodes and photo-conductors [45]. Motivated by the latest progress in coherent microwave-optical interfaces, a potential hardware implementation of a bi-directional optical-to-THz converter for THz CV-QKD was presented in ref. [14]. Hardware realisation of high-efficiency optical-to-THz conversion is challenging and needs to be overcome in the future for practical implementation of THz CV-QKD. The second method is based on direct THz signal generation using quantum cascade lasers using the principle of inter-subband transitions in quantum wells [45, 46]. The challenge here is room temperature operation since some QCLs require cryogenic cooling. Furthermore, for encoding the Gaussian keys on the THz quantum state, efficient electro-optical amplitude and phase modulators operating at THz frequencies are required [15, 47].

5.2 | THz antennas

Once the quantum states are prepared by Alice, efficient directional antennas operating at THz frequencies are required to radiate the quantum EM states towards Bob. Different from macroscopic radio frequency (RF) antennas, carbon nanotubes (CNT) and graphene-based nano-antennas have been proposed for the THz frequency band [48–50]. For coherent state-based THz CV-QKD systems, classical antenna theory is applicable [51]. However, for CV-QKD systems based on squeezed/entangled states, THz antennas need to be designed using the principles of quantum electromagnetics that can maintain both quantum correlations and shape the spatio-temporal characteristics of the EM field [51–53]. Significant technological advances in the hardware realisation of CNT antennas are required for practically realising THz CV-QKD systems.

5.3 | THz detectors

Bob needs to measure the quadrature of the received quantum state using a homodyne or heterodyne detector to extract the raw key information. Since efficient homodyne/heterodyne measurement devices with low electronic noise are readily available for optical frequencies [13], these devices can be used for THz CV-QKD by using a THz-to-optical converter at the receiver [54]. Direct homodyne detection at THz frequencies can also be realised using beamsplitters and plasmonic photo-conductive detectors [15]. Recently, Rydberg atom-based atomic RF sensors have been extensively investigated for accurate RF quadrature measurement [55, 56]. With the advancement in hardware realisation of atomic sensors, direct homodyne/heterodyne detection at THz frequencies is possible in the future [55]. Therefore, THz CV-QKD can be practically implemented by overcoming the hardware realisation challenges of efficient THz-to-optical converters, direct THz homodyne detectors, and THz atomic sensor-based quadrature measurement devices.

6 | CONCLUSIONS AND SUMMARY

This article presents a brief overview of CV-QKD systems operating at microwave and THz frequencies that can provide enhanced security to emerging wireless applications in the quantum world. The THz band provides a sweet spot between high optical frequencies and lower microwave frequencies, having the potential to achieve the best of both worlds. Compared to optical frequencies, THz can work in bad weather conditions while maintaining quantum coherence at room temperatures, which is otherwise not achievable with lower microwave frequencies.

While photonic quantum hardware technology has reached significant maturity [13], quantum hardware is technologically less mature for THz frequencies. This is a major limitation for the implementation of THz CV-QKD systems. However, recently, there has been a significant research focus on developing the different hardware components of THz CV-QKD, including THz signal generators, antennas, and detectors. It is just a matter of time before these components will be integrated together to practically realise a THz CV-QKD system, once sufficient hardware maturity is attained. Tlllhrough this article, we hope to stimulate an interest in the wireless research community to look beyond the classical communication capability of THz frequencies and harness the quantum properties of THz signals for quantum-enhanced security [57].

AUTHOR CONTRIBUTIONS

Neel Kanth Kundu: Conceptualisation; Data curation; Formal analysis; Funding acquisition; Investigation; Methodology; Project administration; Resources; Software; Validation; Visualisation; Writing – original draft; Writing – review & editing. **Matthew R. McKay:** Conceptualisation; Formal analysis; Funding acquisition; Investigation; Methodology; Project administration; Supervision; Validation; Writing – original draft; Writing – review & editing. **Ranjan K. Mallik:** Conceptualisation; Formal analysis; Funding acquisition; Investigation; Methodology; Project administration; Supervision; Validation; Writing – original draft; Writing – review & editing.

ACKNOWLEDGEMENTS

Neel Kanth Kundu acknowledges the support from the INSPIRE Faculty Fellowship awarded by the Department of Science and Technology, Government of India (Reg. No.: IFA22-ENG 344) and the New Faculty Seed Grant from the Indian Institute of Technology Delhi.

Matthew R. McKay acknowledges the support from the Australian Research Council Future Fellowship (project number FT200100928) funded by the Australian Government.

Ranjan K. Mallik acknowledges the support from the Science and Engineering Research Board, a Statutory Body of the Department of Science and Technology, Government of India, under the J. C. Bose Fellowship.

CONFLICT OF INTEREST STATEMENT

The authors declare no conflict of interest.

DATA AVAILABILITY STATEMENT

The data that support the findings of this study are available from the corresponding author upon reasonable request.

ORCID

Neel Kanth Kundu https://orcid.org/0000-0002-6439-4024
Matthew R. McKay https://orcid.org/0000-0002-8086-2545
Ranjan K. Mallik https://orcid.org/0000-0002-0210-5282

REFERENCES

1. Akpakwu, G.A., et al.: A survey on 5G networks for the internet of things: communication technologies and challenges. IEEE Access 6, 3619–3647 (2017). https://doi.org/10.1109/access.2017.2779844
2. Chettri, L., Bera, R.: A comprehensive survey on Internet of Things (IoT) toward 5G wireless systems. IEEE Internet Things J. 7(1), 16–32 (2019). https://doi.org/10.1109/jiot.2019.2948888
3. Liu, R., et al.: Beginning of the journey toward 6G: vision and framework. IEEE Commun. Mag. 61(10), 8–9 (2023). https://doi.org/10.1109/mcom.2023.10298069
4. Gahlot, S., Reddy, S., Kumar, D.: Review of smart health monitoring approaches with survey analysis and proposed framework. IEEE Internet Things J. 6(2), 2116–2127 (2018). https://doi.org/10.1109/jiot.2018.2872389
5. Noel, A.B., et al.: Structural health monitoring using wireless sensor networks: a comprehensive survey. IEEE Commun. Surv. & Tutorials 19(3), 1403–1423 (2017). https://doi.org/10.1109/comst.2017.2691551
6. Lu, X., et al.: Managing physical layer security in wireless cellular networks: a cyber insurance approach. IEEE J. Sel. Area. Commun. 36(7), 1648–1661 (2018). https://doi.org/10.1109/jsac.2018.2825518
7. Wang, Y., Zhang, H., Wang, H.: Quantum polynomial-time fixed-point attack for RSA. China Commun. 15(2), 25–32 (2018). https://doi.org/10.1109/cc.2018.8300269
8. Soni, K.K., Rasool, A.: Cryptographic attack possibilities over RSA algorithm through classical and quantum computation. In: 2018 International Conference on Smart Sylstems and Inventive Technology (ICSSIT), pp. 11–15. IEEE (2018)
9. Raya, A., Mariyappn, K.: Diffie-Hellman instantiations in pre-and post-quantum world: a review paper. In: 2020 Fifth International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN), pp. 130–136. IEEE (2020)
10. Shor, P.W.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Rev. 41(2), 303–332 (1999). https://doi.org/10.1137/s0036144598347011
11. Liu, R., et al.: Towards the industrialisation of quantum key distribution in communication networks: a short survey. IET Quan. Commun. 3(3), 151–163 (2022). https://doi.org/10.1049/qtc2.12044
12. Rozenman, G.G., et al.: The quantum internet: a synergy of quantum information technologies and 6G networks. IET Quan. Commun. 4(4), 147–166 (2023). https://doi.org/10.1049/qtc2.12069
13. Pirandola, S., et al.: Advances in quantum cryptography. Adv. Opt Photon 12(4), 1012–1236 (2020). https://doi.org/10.1364/aop.361502
14. Ottaviani, C., et al.: Terahertz quantum cryptography. IEEE J. Sel. Areas Commun. 38(3), 483–495 (2020). https://doi.org/10.1109/jsac.2020.2968973
15. Liu, X., et al.: Practical aspects of terahertz wireless quantum key distribution in indoor environments. Quan. Inf. Process. 17(11), 1–20 (2018). https://doi.org/10.1007/s11128-018-2068-6
16. He, Y., et al.: Indoor channel modeling for continuous variable quantum key distribution in the terahertz band. Opt. Exp 28(22), 32386–32402 (2020). https://doi.org/10.1364/oe.405020
17. Poor, H.V., Schaefer, R.F.: Wireless physical layer security. Proc. Nat. Acad. Sci. 114(1), 19–26 (2017). https://doi.org/10.1073/pnas.1618130114
18. Fesquet, F., et al.: Perspectives of microwave quantum key distribution in the open air. Phys. Rev. 108(3), 032607 (2023). https://doi.org/10.1103/physreva.108.032607
19. Fesquet, F., et al.: Demonstration of microwave single-shot quantum key distribution. arXiv preprint arXiv:2311.11069 (2023)
20. Han, C., et al.: Terahertz wireless channels: a holistic survey on measurement, modeling, and analysis. IEEE Commun. Surv. & Tutorials 24(3), 1670–1707 (2022). https://doi.org/10.1109/comst.2022.3182539
21. Chen, Z., et al.: A survey on terahertz communications. China Commun. 16(2), 1–35 (2019)
22. Akyildiz, I.F., et al.: Terahertz band communication: an old problem revisited and research directions for the next decade. IEEE Trans. Commun. 70(6), 4250–4285 (2022). https://doi.org/10.1109/tcomm.2022.3171800

23. Sarieddeen, H., Alouini, M.-S., Al-Naffouri, T.Y.: An overview of signal processing techniques for terahertz communications. Proc. IEEE 109(10), 1628–1665 (2021). https://doi.org/10.1109/jproc.2021.3100811
24. Jian, M., Liu, R.: Baseband signal processing for terahertz: waveform design, modulation and coding. In: 2021 International Wireless Communications and Mobile Computing (IWCMC), pp. 1710–1715. IEEE (2021)
25. Casariego, M., et al.: Propagating quantum microwaves: towards applications in communication and sensing. Quantum Sci. Technol. 8(2), 023001 (2023). https://doi.org/10.1088/2058-9565/acc4af
26. Sanz, M., et al.: Challenges in open-air microwave quantum communication and sensing. In: 2018 IEEE Conference on Antenna Measurements & Applications (CAMA), pp. 1–4. IEEE (2018)
27. Renger, M., et al.: Cryogenic microwave link for quantum local area networks. arXiv preprint arXiv:2308.12398 (2023)
28. Zhang, L., et al.: Quantum noise secured terahertz communications. IEEE J. Sel. Top. Quant. Electron. 29(5), 1–10 (2022). Terahertz Photonics. https://doi.org/10.1109/jstqe.2022.3218848
29. Wang, Z., Malaney, R., Green, J.: Inter-satellite quantum key distribution at terahertz frequencies. In: Proc. IEEE Int. Conf. Commun. (ICC). Shanghai, China, pp. 1–7 (2019)
30. Kundu, N.K., et al.: MIMO terahertz quantum key distribution. IEEE Commun. Lett. 25(10), 3345–3349 (2021). https://doi.org/10.1109/lcomm.2021.3102703
31. Kundu, N.K., McKay, M.R.: Channel estimation for reconfigurable intelligent surface aided MISO communications: from LMMSE to deep learning solutions. IEEE Open J. Commun. Soc. 2, 471–487 (2021). https://doi.org/10.1109/ojcoms.2021.3063171
32. Kundu, N.K., et al.: MIMO terahertz quantum key distribution under restricted eavesdropping. IEEE Trans. Quan. Eng. 4, 1–15 (2023). https://doi.org/10.1109/tqe.2023.3264638
33. Weedbrook, C., et al.: Gaussian quantum information. Rev. Mod. Phy. 84(2), 621–669 (2012). https://doi.org/10.1103/revmodphys.84.621
34. Zhang, M., Pirandola, S., Delfanazari, K.: Millimetre-waves to terahertz SISO and MIMO continuous variable quantum key distribution. IEEE Trans. Quan. Eng., 1–11 (2023)
35. Luykx, A., Paterson, K.G.: Limits on Authenticated Encryption Use in TLS (2015). [Online]. https://www.isg.rhul.ac.uk/kp/TLS-AEbounds.pdf
36. Chai, G., et al.: Parameter estimation of atmospheric continuous-variable quantum key distribution. Phys. Rev. 99(3), 032326 (2019). https://doi.org/10.1103/physreva.99.032326
37. Ruppert, L., Usenko, V.C., Filip, R.: Long-distance continuous-variable quantum key distribution with efficient channel estimation. Phys. Rev. 90(6), 062310 (2014). https://doi.org/10.1103/physreva.90.062310
38. Li, Y.: Pilot-symbol-aided channel estimation for OFDM in wireless systems. IEEE Trans. Veh. Technol. 49(4), 1207–1215 (2000). https://doi.org/10.1109/25.875230
39. Yan, H., Yang, H.: Pilot length and channel estimation for massive MIMO IoT systems. IEEE Trans. Veh. Technol. 69(12), 15532–15544 (2020). https://doi.org/10.1109/tvt.2020.3042198
40. Kundu, N.K., McKay, M.R.: A deep learning-based channel estimation approach for MISO communications with large intelligent surfaces. In: 2020 IEEE 31st Annual International Symposium on Personal, Indoor and Mobile Radio Communications, pp. 1–6. IEEE (2020)
41. Pan, Z., et al.: Secret-key distillation across a quantum wiretap channel under restricted eavesdropping. Phys. Rev. App. 14(2), 024044 (2020). https://doi.org/10.1103/physrevapplied.14.024044
42. Wyner, A.D.: The wire-tap channel. Bell Syst. Tech. J. 54(8), 1355–1387 (1975). https://doi.org/10.1002/j.1538-7305.1975.tb02040.x
43. Liu, C., et al.: Multicarrier multiplexing continuous-variable quantum key distribution at terahertz bands under indoor environment and in inter-satellite links communication. IEEE Photon. J. 13(4), 1–13 (2021)
44. Petrov, V.: Frequency down-conversion of solid-state laser sources to the mid-infrared spectral range using non-oxide nonlinear crystals. Prog. Quan. Electron. 42, 1–106 (2015). https://doi.org/10.1016/j.pquantelec.2015.04.001
45. Nagatsuma, T.: Terahertz technologies: present and future. IEICE Electron. Express 8(14), 1127–1142 (2011). https://doi.org/10.1587/elex.8.1127
46. Belkin, M.A., et al.: High-temperature operation of terahertz quantum cascade laser sources. IEEE J. Sel. Top. Quant. Electron. 15(3), 952–967 (2009). https://doi.org/10.1109/jstqe.2009.2013183
47. Ren, Z., et al.: Active and smart terahertz electro-optic modulator based on vo2 structure. ACS Appl. Mater. Interfaces 14(23), 26923–26930 (2022). https://doi.org/10.1021/acsami.2c04736
48. Ren, L., et al.: Collective antenna effects in the terahertz and infrared response of highly aligned carbon nanotube arrays. Phys. Rev. B 87(16), 161401 (2013). https://doi.org/10.1103/physrevb.87.161401
49. Maksimenko, S., et al.: Carbon nanotube antenna: far-field, near-field and thermal-noise properties. Phys. E Low-dimens. Syst. Nanostruct. 40(7), 2360–2364 (2008). https://doi.org/10.1016/j.physe.2007.09.196
50. Wang, R., et al.: Mechanisms and applications of carbon nanotubes in terahertz devices: a review. Carbon 132, 42–58 (2018). https://doi.org/10.1016/j.carbon.2018.02.005
51. Slepyan, G.Y., Vlasenko, S., Mogilevtsev, D.: Quantum antennas. Adv. Quan. Technol. 3(4), 1900120 (2020). https://doi.org/10.1002/qute.201900120
52. Chew, W.C., et al.: Quantum electromagnetics: a new look—part i. IEEE J. multiscale multiphysics Comput. Tech. 1, 73–84 (2016). https://doi.org/10.1109/jmmct.2016.2617018
53. Chew, W.C., et al.: Quantum electromagnetics: a new look—part ii. IEEE J. Multiscale Multiphysics Comput. Tech. 1, 85–97 (2016). https://doi.org/10.1109/jmmct.2016.2614800
54. Ummethala, S., et al.: THz-to-optical conversion in wireless communications using an ultra-broadband plasmonic modulator. Nat. Photon 13(8), 519–524 (2019). https://doi.org/10.1038/s41566-019-0475-6
55. Artusio-Glimpse, A., et al.: Modern RF measurements with hot atoms: a technology review of rydberg atom-based radio frequency field sensors. IEEE Microw. Mag. 23(5), 44–56 (2022). https://doi.org/10.1109/mmm.2022.3148705
56. Anderson, D.A., Sapiro, R.E., Raithel, G.: Rydberg atoms for radio-frequency communications and sensing: atomic receivers for pulsed RF field and phase detection. IEEE Aero. Electron. Syst. Mag. 35(4), 48–56 (2020). https://doi.org/10.1109/maes.2019.2960922
57. Zhou, X., et al.: Towards quantum-native communication systems: new developments, trends, and challenges. arXiv preprint arXiv:2311.05239 (2023)

[Correction added on 5 Sep 2024, after first online publication. The references 3, 5 to 7, 17 and 18, and their citations are deleted from the article.]

How to cite this article: Kundu, N.K., McKay, M.R., Mallik, R.K.: Wireless quantum key distribution at terahertz frequencies: Opportunities and challenges. IET Quant. Comm. 5(4), 450–461 (2024). https://doi.org/10.1049/qtc2.12085