UNIVERSITY of York

This is a repository copy of *Terahertz quantum cryptography*.

White Rose Research Online URL for this paper:
https://eprints.whiterose.ac.uk/159108/

Version: Accepted Version

Article:
Ottaviani, Carlo orcid.org/0000-0002-0032-3999, Woolley, Matthew J., Erementchouk, Misha et al. (4 more authors) (2020) Terahertz quantum cryptography. IEEE Journal on Selected Areas in Communication. pp. 483-495. ISSN 1558-0008

https://doi.org/10.1109/JSAC.2020.2968973

Reuse
Items deposited in White Rose Research Online are protected by copyright, with all rights reserved unless indicated otherwise. They may be downloaded and/or printed for private study, or other acts as permitted by national copyright laws. The publisher or other rights holders may allow further reproduction and re-use of the full text version. This is indicated by the licence information on the White Rose Research Online record for the item.

Takedown
If you consider content in White Rose Research Online to be in breach of UK law, please notify us by emailing eprints@whiterose.ac.uk including the URL of the record and the reason for the withdrawal request.

White Rose university consortium
Universities of Leeds, Sheffield & York

eprints@whiterose.ac.uk
https://eprints.whiterose.ac.uk/

Terahertz quantum cryptography

Carlo Ottaviani,[1] Matthew J. Woolley,[2] Misha Erementchouk,[3] John F. Federici,[4] Pinaki Mazumder,[3] Stefano Pirandola,[1,*] and Christian Weedbrook[5]

[1] *Computer Science & Centre for Quantum Technologies, University of York, YO10 5GH, York, UK*
[2] *School of Engineering and Information Technology, University of New South Wales at the Australian Defence Force Academy, Canberra, ACT 2600, Australia*
[3] *Dept.of Electr. Eng. & Comput. Sci., Univ. of Michigan, Ann Arbor, MI, USA*
[4] *New Jersey Institute of Technology, 323 King Blvd., Newark, NJ 07102*
[5] *Xanadu, 372 Richmond St. W, Toronto, M5V 2L7, Canada*

(Dated: May 10, 2018)

A well-known empirical rule for the demand of wireless communication systems is that of Edholm's law of bandwidth. It states that the demand for bandwidth in wireless short-range communications doubles every 18 months. With the growing demand for bandwidth and the decreasing cell size of wireless systems, terahertz (THz) communication systems are expected to become increasingly important in modern day applications. With this expectation comes the need for protecting users' privacy and security in the best way possible. With that in mind, we show that quantum key distribution can operate in the THz regime and we derive the relevant secret key rates against realistic collective attacks. In the extended THz range (from 0.1 to 50 THz), we find that below 1 THz, the main detrimental factor is thermal noise, while at higher frequencies it is atmospheric absorption. Our results show that high-rate THz quantum cryptography is possible over distances varying from a few meters using direct reconciliation, to about 220m via reverse reconciliation. We also give a specific example of the physical hardware and architecture that could be used to realize our THz quantum key distribution scheme.

arXiv:1805.03514v1 [quant-ph] 9 May 2018

I. INTRODUCTION

The demand for wireless service data rates has increased exponentially in the last decade. However, such a trend is fundamentally limited by Shannon's channel capacity [1]. Beyond this point higher carrier frequencies must be utilized to provide sufficient data rate capacity [2–7]. There are two competing carrier bands for high data rate ($>$ 100 Gb/s) wireless links. The most well-known option is free-space optical communications. The second option is to increase the current wireless carrier technology from the gigahertz range into the terahertz (THz) range and beyond. In fact, while the conventional THz range spans frequencies from 0.1 to 10 THz [8], in this work we consider also the mid infrared (MIR) and far infrared (FIR) frequency range, considering communication channels up to 50 THz.

Both the THz and free-space optical bands have some common features; for instance, both require highly directional beam propagation from the source to the detector. However, one of the most striking and important differences between free-space optical and the THz bands is the practical aspect of weather impact. Atmospheric attenuation, due to ambient humidity and water absorption, limits the maximum link distance achievable at the THz range. However, in the presence of dust, fog, and atmospheric turbulence (scintillation), THz wireless links exhibit very little degradation in performance compared to free-space optical links [9–13]. Under fog conditions, free-space optical links are completely blocked while THz links exhibit minimal impact. Similar transmission windows can be exploited at the MIR and FIR ranges, in particular, between 15 and 34 THz [14].

An important aspect of THz communication is that of achieving the highest levels of security possible where secure distances need to range from 1 m up to 1 km. Applications for secure links include stealthy short distance communications between military personnel and vehicles (manned or unmanned). Security has been considered before in terms of THz communication by exploiting various characteristics and properties of the THz band [2, 3]. Unfortunately, the security of all such 'classical' communication schemes have their limit in the sense that they can never be unconditionally secure. This problem can be fixed by quantum key distribution (QKD) [15, 16]. QKD profits from the peculiar properties of quantum physics and quantum information [17, 18], in particular the no-cloning theorem [19] and the monogamy of entanglement [20], to achieve levels of security that are not possible using classical cryptography.

Continuous-variable (CV) QKD [16, 21, 22] has attracted increasing attention in the last years. This is due to the high rates achievable that allow one to approach the ultimate limit of point-to-point private communication [23–25], i.e., the PLOB bound [23], equal to $-\log_2(1-T)$ secret bits per transmission over a bosonic pure-loss channel with transmissivity T. Several CV-QKD protocols have been proposed relying on one-way [26–29], and two-way communication [30–33], measurement-device-independence [34] and exploiting entanglement in the middle [35]. Several experimental tests [36, 40, 41] have shown the capacity of CV-

*Electronic address: stefano.pirandola@york.ac.uk

QKD to achieve high-rate secure communication over metropolitan distances [42] and beyond [43]. Recent studies focused on improving the achievable distance by Gaussian post-selection [44, 45], exploiting noiseless linear amplifier [46], and also refining the performance of classical error correction and privacy amplification stages [47, 48]. Others works have shown the feasibility of CV-QKD at wavelengths longer than optical down to the microwave regime [37–39], also incorporating finite-size effects [49]

In this work, we study the feasibility of CV-QKD at the terahertz and the extended teraherz range, i.e., from 100 GHz to 50 THz. We assume directional beam propagation, and the best communication windows available that are between 15 to 34 THz. We consider asymptotic key rates under collective Gaussian attacks [50–52], which represent the optimal eavesdropping [53] after de Finetti symmetrization [54, 55]. In particular, we consider single-mode Gaussian attacks that are optimal [56] in the context of one-way protocols, while two-mode strategies [31] are typically more effective against two-way quantum communications [57] and measurement-device-independent protocols. In addition to this, we give a specific description of the hardware for the optical-THz conversion, inspired by techniques based on the coupling of microwave and optical fields [58, 59] to phonons of a mechanical resonator [60, 61].

The structure of this paper is the following. In Sec. II, we introduce the communication protocol at THz frequency, we describe the encoding mechanism and the general aspects of the security analysis. In Sec. III, we study the performances of THz QKD. In Sec. IV, we describe the hardware implementation of the optical-to-terahertz frequency conversion. Finally, Sec. V is left to discussions and conclusions.

II. TERAHERTZ QKD

In this section we describe the THz QKD scheme for Gaussian encoding, along with the corresponding secret key rates. We assume an eavesdropping where the injected thermal noise matches the amount of trusted thermal noise used by the encoder [37, 38].

A. Encoding

The encoding of a protocol for THz QKD is based on the Gaussian modulation [26] of thermal states, as also typical in other studies of QKD at different wavelengths [37–39]. It goes as follows: Alice randomly displaces the two quadratures, q and p, of a quantum THz source state (thermal state) according to a bivariate zero-mean Gaussian distribution. She does this many times, sending each displaced signal state to the receiver (Bob), over an insecure quantum channel. The latter can be realistically modelled as a Gaussian thermal-loss channel [16] with transmissivity T and thermal variance W.

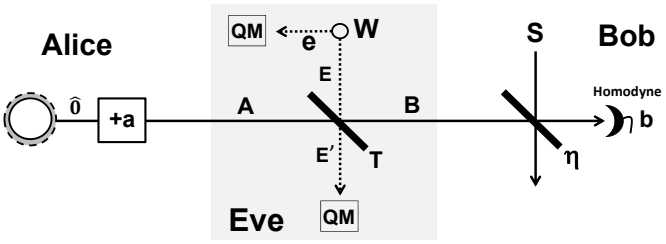

FIG. 1: THz QKD protocol with noisy (i.e., realistic) homodyne detection. Alice prepares thermal THz states by displacing their generic quadarature $\hat{0}$ by some Gaussian variable a. She then sends the displaced states through a thermal-loss channel which is controlled by Eve. This channel can be described as a beam splitter with transmissivity T subject to thermal noise variance W. This noise is produced by mode E of a two-mode squeezed vacuum (TMSV) state with variance W. Eve's output modes e and E' are stored in a quantum memory (QM) and coherently detected by Eve at the end of all the communication (collective entangling cloner attack). At the detection stage, Bob randomly switches the setup of his homodyne detection, measuring quadrature q or p. Bob's output variable is denoted by b. The beam splitter η describes the efficiency of the detector, which is also subject to trusted thermal noise with variance S. We study the performance of the protocol for several values of the efficiency, assuming $\eta = 10\%$ in a realistic implementation.

At the output of the channel, Bob measures the incoming thermal states by using a THz shot-noise-limited quantum detector; this consists of a noisy homodyne detection which is randomly switched between the q- and the p- quadrature. As depicted in Fig. 1, Bob's detection can be described as a beam splitter with transmissivity η (mimicking the detector efficiency) before an ideal homodyne detector. One input port is fed with the incoming signals, while at the other input is subject to trusted thermal noise with variance S. The detection is followed by steps of classical post-processing which allows Alice and Bob to extract a perfectly-correlated bit string. This is the secret key which can be used to encrypt confidential messages via the one-time pad.

We can describe Alice's mode with the generic quadrature operator $A = \hat{0} + a$, having total variance $V_A = V_0 + V_a$. Here a is a real number used to denote Alice's classical encoding variable with a variance of V_a. Now $\hat{0}$ is the 'THz quadrature operator' which can be thought of as the thermalness of the quantum modes due to the background thermal noise at the THz frequencies [37]. This mode has a corresponding variance given by V_0, the 'terahertz parameter', defined as $V_0 := 2\bar{n}+1$, where 1 is the vacuum shot noise unit (SNU) and $\bar{n}$ is the mean thermal photon number. The latter is obtained from Planck's black-body formula $\bar{n} = [\exp(h\omega/k_B t) - 1]^{-1}$, where t is the temperature (here assumed to be 296 K), h is Planck's constant, k_B is Boltzmann's constant, and ω is the frequency.

The range of frequencies considered in this work goes from 100 GHz, for which we have $V_0 = 123.3$ SNU, to 50 THz ($V_0 \simeq 1.001$ SNU). Bob's measurement device extracts the best estimate of Alice's variable a. Specifically, this is achieved by using a shot-noise-limited THz homodyne detector that randomly switches between the two quadratures. Bob's corresponding output variable is denoted by b. Unlike previous schemes [37–39], here we also take into account and analyze the effect of a realistic detector at Bob's side.

B. Security of terahertz quantum cryptography

We will now discuss the eavesdropping strategy against the THz QKD protocol. First, note that all the elements of the protocol are Gaussian [16], i.e., the source state is Gaussian and the detection is Gaussian. It is known that the most powerful attacks against Gaussian protocols are Gaussian, whose general form has been characterized in Ref. [52]. In particular, this attack can be assumed to be collective under a suitable symmetrization in the limit of large key length [50, 51, 55]. The most important and practical implementation of this attack is a collective entangling cloner attack [62]. This is described in Fig. 1, where a beam splitter with transmissivity T simulates the channel attenuation. Then the thermal noise W is simulated by injecting part of a two-mode squeezed state (TMSV), which is a zero mean Gaussian two-mode state $\Phi_{eE}(W)$ with covariance matrix (CM)

$$\mathbf{V}_{eE} = \begin{pmatrix} W\mathbf{I} & \sqrt{W^2-1}\mathbf{Z} \\ \sqrt{W^2-1}\mathbf{Z} & W\mathbf{I} \end{pmatrix}, \tag{1}$$

where $\mathbf{I} := \mathrm{diag}(1,1)$ and $\mathbf{Z} := \mathrm{diag}(1,-1)$. According to Fig. 1, the output ancillas e and E' are stored in a quantum memory and measured by the eavesdropper (Eve) after Alice and Bob finish the classical communication stage. To quantify the amount of information gained by Eve, it is then sufficient to study the total output CM $V_{eE'}$ and the conditional CMs $V_{eE'|a}$ and $V_{eE'|b}$, depending on the variable (a or b) used for the reconcilation.

Let us remark a peculiarity of Eve's attack against a thermal protocol at lower frequencies, compared to a convential protocol working at optical or telecom wavelengths (1550 nm). In the optical range, we can set $V_0 = 1$ SNU for the signal states (coherent states). At frequencies lower than the optical ones, the shot-noise level of Bob's detector is larger than 1 SNU and this is equal to the preparation noise V_0. For this reason, Eve may potentially hide herself in this background noise [37, 38]. For any attenuation T introduced in the communication line, she can compensate for the reduction of the preparation noise TV_0 by additing a thermal noise $W = V_0$, so that Bob's detector still gets the same shot-noise level $TV_0+(1-T)W = V_0$. Because the value of V_0 can become very large at lower frequencies (e.g., below 1 THz), this means that Eve may simulate the environmental noise with a highly-entangled TMSV state $\Phi_{eE}(W)$ which is therefore very destructive and represents the main bottleneck for long-distance implementations.

In order to avoid this problem, Bob's detector should be able to filter the background noise. However, this approach increases the complexity of the protocol and seems to require the use of entanglement at the input source. For instance, in quantum illumination [63–67], the use of entangled photons allows the receiver to distinguish the reflected signal photon (still quantum-correlated with a corresponding idler photon) from the background of uncorrelated thermal photons. Thanks to this "labeling", quantum illumination works very well at the microwave frequencies, therefore providing a basic mechanism for quantum radar [67]. This quantum illumination approach was adopted for private communication in noisy conditions [68, 69] but, as mentioned above, it requires a two-way protocol based on the use of quantum entanglement at the input.

C. Secret key rates

The security performance of the protocol is assessed by computing key rate R in the asymptotic regime. Depending on which variable, a or b, the parites reconciliated their data, we have direct reconciliation (DR) [26] or the reverse reconciliation (RR) [27]. The definitions of the key rate in DR ($\blacktriangleright$) and RR ($\blacktriangleleft$) is given by the following formulas

$$R^{\blacktriangleright} := I(a:b) - I(E:a), \tag{2}$$

$$R^{\blacktriangleleft} := I(a:b) - I(E:b), \tag{3}$$

where $I(a:b)$ is Alice and Bob's mutual information, while $I(E:a)$ and $I(E:b)$ are Eve's accessible information with respect to the variable a and b, respectively. These are bounded by the Holevo information [70, 71] $\chi^{\blacktriangleright} = \chi(E:a)$ in DR, and $\chi^{\blacktriangleleft} = \chi(E:b)$ in RR.

Recall that the Holevo information χ is defined as

$$\chi := H - H_c, \tag{4}$$

where H (H_c) is the von Neumann entropy of Eve's total (conditional) state [16]. For a Gaussian state ρ, the von Neumann takes the simple expression

$$H = \sum_x h(x), \tag{5}$$

where $x \geq 1$ are the symplectic eigenvalues of the CM associated with ρ, and

$$h(x) := \frac{x+1}{2}\log_2\frac{x+1}{2} - \frac{x-1}{2}\log_2\frac{x-1}{2}. \tag{6}$$

The total von Neumann entropy H is obtained first by computing the CM $\mathbf{V}_{eE'}$ of Eq. (A7), corresponding to Eve's output state $\rho_{eE'}$. From $\mathbf{V}_{eE'}$ it is simple to obtain the pair of symplectic eigenvalues (see Appendix A

for details). In the asymptotic limit of high modulation ($V_a \gg 1$), the total von Neumann entropy is given by

$$H = h\left(W\right) + \log_2 \frac{e}{2}(1-T)V_a \tag{7}$$

To study DR we compute the conditional CM $\mathbf{V}_{eE'|a}$ from which one obtains the corresponding von Neumann entropy $H_c^{\blacktriangleright}$ for Eve's output state conditioned to Alice's encoding, i.e., $\rho_{eE'|a}$. After some algebra, one obtains the following asymptotic expression

$$H_c^{\blacktriangleright} = h(\bar{\nu}_1) + \frac{1}{2}\log_2 \frac{e^2}{4}(1-T)\Lambda(W,V_0)V_a, \tag{8}$$

where

$$\Lambda(x,y) := Tx + (1-T)y, \tag{9}$$

and the explicit expression of the eigenvalue $\bar{\nu}_1$ is given in Eq. (A12) of Appendix A.

For RR we only need to compute the CM describing Eve's output state conditioned to Bob's variable b, i.e., $\rho_{eE'|b}$. This is obtained by completing the CM $\mathbf{V}_{eE'}$ with the entries describing Bob's mode b and its correlation with Eve's output modes. Then we apply homodyne detection to Bob's mode b, to obtain the conditional CM $\mathbf{V}_{eE'|b}$, whose explicit expression is given in Eq. (A20) of Appendix A. From $\mathbf{V}_{eE'|b}$, we compute the conditional symplectic spectrum and, taking the asymptotic limit, we derive the following conditional von Neumann entropy

$$H_c^{\blacktriangleleft} = h\left(\bar{\nu}_3\right) + \frac{1}{2}\log_2 \frac{e^2}{4}\frac{(1-T)\left[S\left(1-\eta\right)\left(1-T\right)+W\eta\right]}{T\eta}V_a, \tag{10}$$

where the explicit expression of the symplectic eigenvalue $\bar{\nu}_3$ can be found in Appendix A 3.

Using the expression for the Alice and Bob's mutual information

$$I(a:b) = \frac{1}{2}\log_2 \frac{\eta T V_a}{\eta T V_0 + \eta(1-T)W + (1-\eta)S}, \tag{11}$$

whose derivation is detailed in Appendix A, we obtain the following key rate in DR

$$R^{\blacktriangleright}(V_0,T,W,\eta,S) = h\left[\sqrt{\frac{W\Lambda(1,WV_0)}{\Lambda(W,V_0)}}\right] - h(W) + \frac{1}{2}\log_2 \frac{T\eta\Lambda(W,V_0)}{(1-T)[\eta\Lambda(V_0,W)+(1-\eta)\,S]}, \tag{12}$$

and the following one in RR

$$R^{\blacktriangleleft}(V_0,T,W,\eta,S) = h\left(\bar{\nu}_3\right) - h\left(W\right) + \frac{1}{2}\log_2 \frac{(1-\eta)\left(1-T\right)S + W\eta}{(1-T)[\eta\Lambda(V_0,W)+(1-\eta)S]}. \tag{13}$$

III. PERFORMANCES IN THE EXTENDED TERAHERTZ RANGE

In this section, we study the perfomances of the key rates in DR and RR. In particular, in subsection III A, we plot the secret-key rates and the security thresholds, while in subsection III B we express the security thresholds in terms of maximally-achievable frequencies versus channel transmissivity. We assume a collective entangling-cloner attack where Eve hides in the detection/preparation noise $W = V_0$. Then, in order to optimize the protocol, one can check that the DR rate in Eq. (12) is maximized by $S = 1$, so that we may write

$$R^{\blacktriangleright}(V_0,T,\eta) = h\left[\sqrt{T+(1-T)V_0^2}\right] - h(V_0) + \frac{1}{2}\log_2 \frac{T\eta V_0}{(1-T)(\eta V_0+1-\eta)}. \tag{14}$$

For the RR rate in Eq. (13), we consider both the absence of trusted noise ($S = 1$) and its presence by setting $S = V_0$. Therefore, our rate is the maximum

$$R^{\blacktriangleleft}(V_0,T,\eta) := \max\{R^{\blacktriangleleft}(V_0,T,V_0,\eta,1), R^{\blacktriangleleft}(V_0,T,V_0,\eta,V_0)\}, \tag{15}$$

where

$$R^{\blacktriangleleft}(V_0,T,W=V_0,\eta,S=1) = h\left[\sqrt{\frac{\left[(1-T)\left(1-\eta\right)+\eta\right]V_0}{(1-T)\left(1-\eta\right)+V_0\eta}}\right] - h\left(V_0\right) + \frac{1}{2}\log_2 \frac{(1-\eta)\left(1-T\right)+V_0\eta}{(1-T)[\eta V_0+1-\eta]}, \tag{16}$$

and

$$R^{\blacktriangleleft}(V_0,T,W=V_0,\eta,S=V_0) = h\left[\sqrt{\frac{(1-T)\left(1-\eta\right)V_0+\eta}{(1-T)\left(1-\eta\right)+\eta}}\right] - h\left(V_0\right) + \frac{1}{2}\log_2 \eta\left(1-\eta\right) - \frac{1}{2}\log_2(1-T). \tag{17}$$

Now notice that the preparation noise V_0 is uniquely determined by the frequency ω (at fixed temperature $t \simeq 296$ K), so that we may set $R = R(\omega,T,\eta)$ in the previous formulas. Then, solving the equation $R(\omega,T,\eta) = 0$ provides the security threshold $\omega = \omega(T,\eta)$ in terms of minimum-tolerable or accessible frequency versus transmissivity T and detector efficiency η. In the following section, we study the behavior of the rates in DR and RR, finding an optimal frequency at $\omega_{\max} = 30$ THz. We then compare these optimal rates with the PLOB upper-bound, which is computed for a thermal-loss channel [23] with transmissivity T and thermal noise $W = V_0(\omega)$ determined by the optimal frequency $\omega_{\max} = 2\bar{n}_{\max} + 1$. This upper-bound takes the analytical form

$$\mathcal{B} = -\log_2[(1-T)T^{\bar{n}_{\max}}] - h[V_0(\omega_{\max})], \tag{18}$$

for $\bar{n}_{\max} < T(1-T)^{-1}$, while $\mathcal{B} = 0$ otherwise.

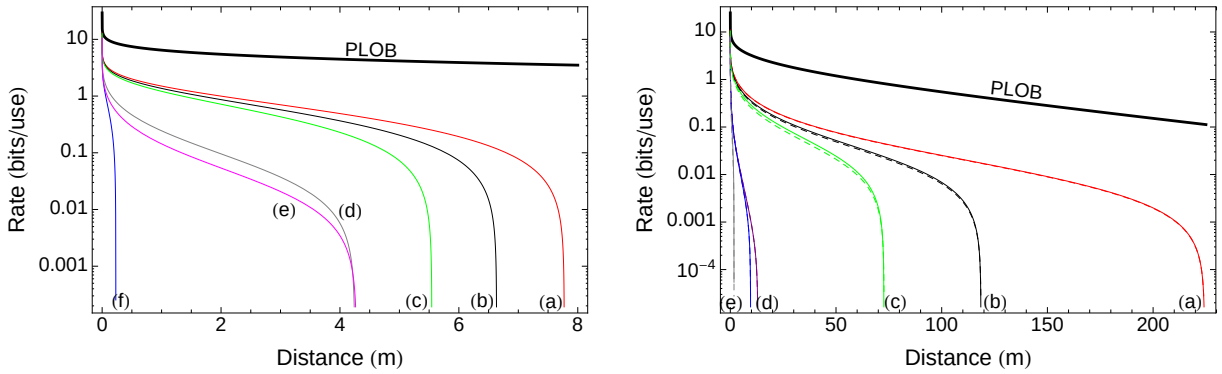

FIG. 2: (Color online) Secret-key rates (bits/use) versus distance (m) assuming a detection efficiency $\eta = 10\%$. The **left** panel refers to DR. The curves are as follows: (a) 30 THz, (b) 20 THz, (c) 15 THz, (d) 100 GHz, (e) 200 GHz, and (f) 40 GHz. We also show the PLOB upper bound $\mathcal{B}$ for a thermal-loss channel which is computed assuming the parameters of the optimal curve (a). For each curve we have a specific value of δ [8, 14], playing a crucial role in the achievable distance. We have $\delta = 50$ dB/Km for $15 - 34$ THz, therefore for curves (a), (b) and (c) (and the PLOB bound). For ω in the range $40 - 55$ THz, we have $\delta = 1.77 \times 10^3$ dB/Km. From 100 GHz to 10 THz, there are several transmission windows, within a generally rising atmospheric absorption: At 100 GHz $\delta = 0.6$ dB/Km, at 200 GHz $\delta = 1.2$ dB/Km, at 1 THz $\delta = 10^2$ dB/Km, while at 10 THz $\delta = 10^3$ dB/Km. The **right** panel refers to RR. The curves are as follows: (a) 30 THz, (b) 20 THz, (c) 15 THz, (d) 50 THz (purple line) and 40 THz (blue line), (e) 10 THz. Here too we show the PLOB upper bound $\mathcal{B}$ for a thermal-loss channel.

A. Behaviour of the secret key rates

Let us analyse the behaviour of the previous rates $R = R(\omega, T, \eta)$. We assume detection efficiency $\eta = 10\%$ and, for several frequencies ω, we study the behaviour of the rate R versus distance d (km) by setting $T = 10^{-\frac{\delta d}{10}}$, where δ describes the atmospheric loss (dB/km). As shown in the left panel of Fig. 2, we find that the best performance of the DR rate $R^{\blacktriangleright}$ is obtained for the frequency range $15 - 34$ THz. In particular, the optimal key rate occurs at $\omega = 30$ THz and follows the scaling of the PLOB bound $\mathcal{B}$ until about 200 m. This result shows that THz QKD is possible in DR, with a key rate of 10^{-3} (bit per use) over short distances of order of meters, despite the low detector efficiency η. Then, in the right panel of Fig. 2, we see that the best performance of the RR rate $R^{\blacktriangleleft}$ is also achieved at $\omega = 30$ THz, which may allow a secret-key rate of 10^{-4} bit/use over a distance of about 220 m.

There are two features that mainly deteriorate the performance: one is the large thermal background that demands to consider entangling cloner attacks with increasingly large thermal variance $W = V_0(\omega)$, as we move to the low frequency range of the electromagnetic spectrum. The other is the atmospheric absorption condition that, after starting very low in the microwave range ($\omega < 100$ GHz), grows exponentially as we move towards higher frequencies. The atmospheric attenuation is caused by the increasing coupling of the electromagnetic signals with the gases and molecules composing the atmosphere and may even varying drastically, depending on the weather conditions [8, 14].

For the sake of simplicity we assume attenuation under fairly clear atmospheric conditions noticing that, even in this case, it can vary considerably from $\delta = 0.6$ dB/km at 100 GHz to $\delta = 10^2$ dB/km at 1 THz to arrive to $\delta = 10^3$ dB/km at 10 THz. After this range of frequencies absorption decreases and several transmission windows become available, for instance between 15 and 34 THz, where the loss rate is estimated to be around $\delta = 50$ dB/km, under pristine conditions [14]. Then, the attenuation rises again for frequencies above this range, but less sharply than before: at 50 THz we have again losses as high as approximately $\delta = 1.77 \times 10^3$ dB/km.

B. Accessible frequencies

Let us now study the security threshold expressed in terms of accessible frequencies versus channel transmissivity and detector efficiency, i.e., $\omega = \omega(T, \eta)$. This analysis follows and extends a similar approach described in Refs. [37–39]. We show the performance in DR and RR, and we also compare it with the threshold coming from the PLOB upper bound $\mathcal{B} = 0$, which is equal to $\bar{n} = T(1 - T)^{-1}$, i.e.,

$$\omega = \frac{1 + T}{1 - T}. \tag{19}$$

In Fig. 3 positive rates are those *above* the thresholds. As we can see there is a window of positive rates opening already at 1 THz according to the PLOB bound. However, our protocols start to work well (in both DR and RR) from about 10 THz, where wide ranges of transmissivities are accessible.

In particular, note that the RR security threshold $\omega^{\blacktriangleleft} = \omega^{\blacktriangleleft}(T, \eta)$, coming from $R^{\blacktriangleleft} = 0$, is computed assuming detection efficiency $\eta = 10\%$. This efficiency can

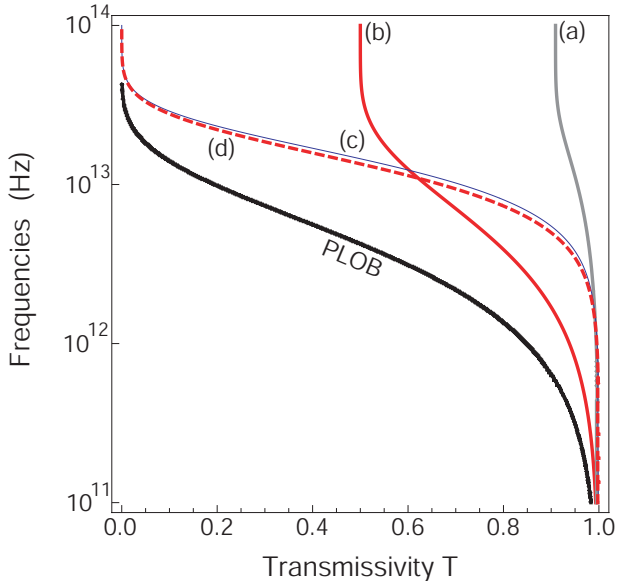

FIG. 3: (Color online) Security thresholds in terms of accessible frequencies ω (Hz) versus channel transmissivity T. Regions *above* the thresholds are secure. The curves are: (a) DR with $\eta = 10\%$, (b) DR with $\eta = 100\%$, (c, solid blue) RR with $\eta = 100\%$, (c, dashed red) RR with $\eta = 10\%$ and detector's trusted noise $S = V_0$. We compare these results with the threshold associated with the PLOB bound of Eq (19).

be obtained as a two-step operation by combining a preliminary conversion from the THz frequencies to optical, followed by an optical homodyne detection, which can be performed with nearly unit efficiency [72, 73]. Therefore the overall efficiency η is limited by the efficiency $\tilde{\eta}$ of the THz-optical conversion. Recent works [58, 61] suggests that it is reasonable to set this efficiency $\tilde{\eta} = 10\%$. In the following section, we describe a possible hardware realization for a coherent THz-optical converter.

IV. PHYSICAL HARDWARE REALIZATION

Terahertz sources, modulators and detectors (see Fig. 4 (a)) are substantially less well-developed than their optical counterparts. Here we sketch a hardware realization of a terahertz quantum communication system based on coherent terahertz-optics conversion and existing optical technology. In particular, we describe the operation of a coherent terahertz-optical interface, mediated via a low-frequency mechanical resonance. This approach for THz QKD is motivated by recent progress in the development of coherent microwave-optical interfaces [58, 74, 75] which can be used to create a hybrid quantum network [76–78]. Such interfaces operate via the coupling of microwave and optical fields to a common phononic mode in a solid-state material.

The proposed bidirectional terahertz-optical converter (see Fig. 4 (b)) consists of a THz and optical cavity mode,

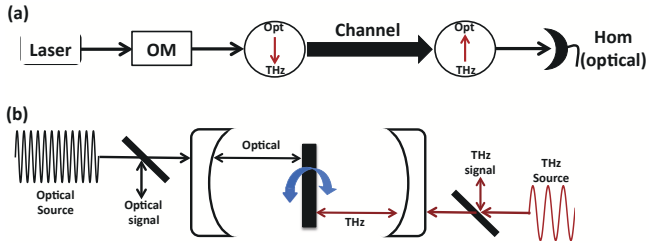

FIG. 4: (Color online) Potential hardware implementation of a THz-optical converter. (a) Optical signals generated by a laser are optically modulated (OM) and then converted from optical frequencies to THz. The THz signals are sent through the channel, and their outputs are converted back to optical. Finally, Bob performs an optical homodyne detection (hom). Note that the attenuation of the first optical-to-THz conversion can be mitigated by increasing the input power level before the converter. (b) We show how a THz-optical converter could work, exploiting the mediation via a common mechanical mode. The cavities are schematically represented as Fabry-Perot, but also implementation based on co-locating optical, THz and phonon modes in photonic/phononic crystals could be considered. Co-location of optical and phonon modes has been proved in Ref. [80], as well as photonic crystals implementation [81].

each coupled to a common (linearized) phononic mode, and out-coupled to a THz and optical waveguide, respectively. The phononic mode is sideband-coupled to both the THz and the optical cavity modes. The terahertz and optical cavity mode resonance frequencies are denoted by ω_t and ω_0, and the decay rates into the coupled waveguide modes are denoted by κ_t and κ_0, respectively. The phononic mode frequency is denoted by ω_m, and its effective coupling rates to the terahertz and optical cavity modes are given by g_t and g_0, respectively.

This device may be analyzed using the input-output theory of quantum optics [79], as described in detail in Appendix B. Denoting the quadrature frequency components of the optical input and output fields by $q_{o,in/out}[\omega]$ and of the terahertz input and output fields by $q_{t,in/out}[\omega]$, the terahertz-optical and optical-terahertz frequency-dependent transmissivity may be defined by

$$t(\omega) = \frac{\langle q_{o,out}(\omega)\rangle}{\langle q_{t,in}(\omega)\rangle} = \frac{\langle q_{t,out}(\omega)\rangle}{\langle q_{o,in}(\omega)\rangle}, \tag{20}$$

where ω is defined with respect to ω_t (ω_o) for the terahertz (optical) mode. It may be shown that the zero-frequency transmissivity is given by

$$|t(\omega = 0)| = \frac{8 g_o g_t \sqrt{\kappa_o \kappa_t}}{4(g_o^2 \kappa_t + g_t^2 \kappa_o) + \kappa_o \kappa_m \kappa_t}. \tag{21}$$

This transmissivity goes to one in the limit of negligible damping $\kappa_m \to 0$, symmetric couplings $g_o = g_t = g$, and symmetric out-couplings $\kappa_o = \kappa_t = \kappa$.

Now for high-fidelity conversion, in addition to a near-unity zero-frequency gain, the converter must also have a

flat magnitude response and a linear phase response over a reasonable bandwidth. As detailed in Appendix B, this would be the case over a range of frequencies ω such that

$$|\omega| \ll g, \kappa, 4g^2/\kappa. \tag{22}$$

This might lead to a useful modulation bandwidth of the order of $\sim 10\,\mathrm{MHz}$, sufficient for the required coherent field modulation.

V. DISCUSSION AND CONCLUSION

In this work, we have studied the feasibility of quantum cryptography working in the THz range of frequency of the electromagnetic spectrum, going from 0.1 to 50 THz. This frequency range is attractive for the potential boosting of data rate of wireless communication. To perform this study we assumed unidirectional, plane-wave emission setup, and we performed the security analysis in the asymptotic limit of many uses of the quantum channel, bounding the eavesdropper's accessible information by the Holevo bound. We focused on a switching protocol, where the receiver decoding is performed by randomly switching between the two possible quadratures to homodyne. We assumed detections performed in the THz range with an efficiency of 10%, which represents the performance of recent optical-to-microwave conversion rate and state-of-the-art THz devices [58, 61, 74, 75, 80].

We found that QKD at THz frequencies is possible in both direct and reverse reconciliation, over short distances, because of the following trade-off: THz radiation is strongly affected by atmospheric loss, caused by suspended molecules in atmosphere, which sharply increase losses as we move away from the microwave regime. By contrast moving towards the microwave regime, we have to deal with a large thermal background. This second aspect is particularly harmful for signals below 1 THz, where the thermal background is already more than one order-of-magnitude higher than the vacuum noise. The eavesdropper can exploit this high level of shot noise for her attack.

The range of distances over which it is possible to implement THz QKD is indeed short, if compared to optical communication. In particular, we found that in direct reconciliation we can achieve a key rate of 10^{-2} bit/use over a distance of meters, about 4 m at 0.1 THz and 7.5 m at 30 THz. This can be used for short-range applications, such as credit card/ATM transactions or proximity and access cards, e.g., for secure access of buildings. Then, using reverse reconciliation at 30 THz, we obtain a key rate of 10^{-3} bit/use, over a distance of about 220 m.

The analysis of the security thresholds at various frequencies, summarized in Fig. 3, shows that direct reconciliation is limited to high-transmission conditions, mainly as a consequence of the low-efficiency of 10% of Bob's detector. By contrast, reverse reconciliation is less affected by the low detector efficiency and it is possible to obtain a positive key at transmissivity as low as $T \simeq 0.1$. In addition to this, the use of trusted-noise-assisted detection helps to increase the security threshold, despite the fact that the benefit is incremental.

In conclusion, we have explored the possibility of implementing quantum cryptography in the THz regime, finding that this is possible over short distances with suitably high rates. The distance range depends crucially on the transmission windows considered. Further analysis may take into account the impact of finite-size effects, and the possibility of using other communication protocols, like two-way schemes. Let us also remark that working in the THz range of frequencies can also provide some technical advantage with respect to the standard optical regime. At optical frequencies, an intense oscillator signal is typically used to keep synchronized the phases of Alice's and Bob's systems. By contrast, at much lower frequencies as the THz ones, we may use local clocks to mantain the relative phase of the quadratures.

VI. ACKNOWLEDGEMENTS

We thank Michael Leuenberger for discussions. CO and SP acknowledge support from the EPSRC via the 'UK quantum communications hub' (Grant no. EP/M013472/1).

Appendix A: Details of the computation of the secret-key rates

1. Mutual information

We begin the security analysis by noting that, at Bob's side, the loss and noise affecting his detector can be modeled by a beam splitter with transmission η processing the incoming mode with a trusted mode with variance S an part of a TMSV with CM

$$\mathbf{V}_S = \begin{pmatrix} S\mathbf{I} & \sqrt{S^2-1}\mathbf{Z} \\ \sqrt{S^2-1}\mathbf{Z} & S\mathbf{I} \end{pmatrix}. \tag{A1}$$

The first quantity to calculate is the mutual information between Alice and Bob $I(a:b)$, which is identical for both DR and RR. It is defined as

$$I(a:b) = \frac{1}{2}\log_2 \frac{V_b}{V(b|a)} \tag{A2}$$

where V_b is the variance of Bob's output mode b and is given by

$$V_b = \eta T V_A + \eta(1-T)W + (1-\eta)S. \tag{A3}$$

The conditional variance is instead given by

$$V(b|a) = \eta T V_0 + \eta(1-T)W + (1-\eta)S. \tag{A4}$$

Therefore, using Eq. (A3) and Eq. (A4), we may write Alice and Bob's mutual information

$$I(a:b) = \frac{1}{2}\log_2 \frac{\eta T V_A + \eta(1-T)W + (1-\eta)S}{\eta T V_0 + \eta(1-T)W + (1-\eta)S}. \tag{A5}$$

This expression simplifies in the asymptotic limit of large signal modulation $V_a \gg 1$, where it becomes

$$I(a:b) \to \frac{1}{2}\log_2 \frac{\eta T V_a}{\eta T V_0 + \eta(1-T)W + (1-\eta)S}. \quad \text{(A6)}$$

2. Direct Reconciliation

The CM of Eve's output modes e and E' is given by

$$\mathbf{V}_{eE'} = \begin{pmatrix} W\mathbf{I} & \sqrt{T(W^2-1)}\mathbf{Z} \\ \sqrt{T(W^2-1)}\mathbf{Z} & TW + (1-T)V_A\mathbf{I} \end{pmatrix}. \quad \text{(A7)}$$

In the limit of large modulation ($V_a \gg 1$), we can compute its symplectic spectrum by finding the eigenvalues of $\nu = |i\Omega V_b|$ [16], which are

$$\nu_1 \to W \quad \text{(A8)}$$

$$\nu_2 \to (1-T)V_a. \quad \text{(A9)}$$

Consequently, we find that Eve's entropy is given by

$$H = h(\nu_1) + h(\nu_2) \to h(W) + \log\frac{e}{2}(1-T)V_a, \quad \text{(A10)}$$

where

$$h(x) := \frac{x+1}{2}\log_2\frac{x+1}{2} - \frac{x-1}{2}\log\frac{x-1}{2}. \quad \text{(A11)}$$

Eve's conditional CM $\mathbf{V}_{eE'|a}$ can be computed by setting $V_a = 0$ in matrix $\mathbf{V}_{eE'}$, given in Eq. (A7), for one of the two quadratures. The corresponding asymptotic symplectic eigenvalues are then given by

$$\bar{\nu}_1 \to \sqrt{\frac{W\Lambda(1, WV_0)}{\Lambda(W, V_0)}}, \quad \text{(A12)}$$

$$\bar{\nu}_2 \to \sqrt{(1-T)\Lambda(W, V_0)V_a}\,, \quad \text{(A13)}$$

where we define $\Lambda(x,y) := Tx + (1-T)y$. Eve's conditional entropy is therefore given by

$$H_c^{\blacktriangleright} \to h(\bar{\nu}_1) + \log\frac{e}{2}\sqrt{(1-T)\left[TW + (1-T)V_0\right]V_a}\,. \quad \text{(A14)}$$

Using Eqs. (A10) and (A14), Eve's Holevo information is given by

$$\chi(E:a) = H - H_c^{\blacktriangleright} \to h(W) - h(\bar{\nu}_1) + \frac{1}{2}\log\frac{(1-T)V_a}{\Lambda(W,V_0)}\,. \quad \text{(A15)}$$

By using Eq. (A15) and Eq. (A5) we can write the final key rate as

$$R^{\blacktriangleright}(V_0,T,W,\eta,S) = \frac{1}{2}\log\frac{T\eta\Lambda(W,V_0)}{(1-T)[\eta\Lambda(V_0,W) + (1-\eta)\,S]} + h\left[\sqrt{\frac{W\Lambda(1,WV_0)}{\Lambda(W,V_0)}}\right] - h(W)\,, \quad \text{(A16)}$$

which is given in Eq. (12) of the main text.

3. Reverse Reconciliation

Note that Eve and Bob's joint CM is given by

$$\mathbf{V}_{eE'B} = \begin{pmatrix} \mathbf{V}_E & \mathbf{C} \\ \mathbf{C}^T & \mathbf{B} \end{pmatrix}, \quad \text{(A17)}$$

where

$$\mathbf{B} = \eta[\Lambda(V_0,W) + TV_A + ((1-\eta)/\eta)S]\mathbf{I}, \quad \text{(A18)}$$

and

$$\mathbf{C} = \begin{pmatrix} \sqrt{\eta(1-T)(W^2-1)}\mathbf{Z} \\ \sqrt{\eta T(1-T)}(W-V_A)\mathbf{I} \end{pmatrix}. \quad \text{(A19)}$$

Because Bob uses homodyne detection, Eve's conditional covariance matrix is given by

$$\mathbf{V}_{eE'|\beta} = \mathbf{V}_{eE'} - \mathbf{C}(\mathbf{\Pi}\mathbf{B}\mathbf{\Pi})^{-1}\mathbf{C}^T, \quad \text{(A20)}$$

where $\mathbf{\Pi} := \mathrm{diag}(1,0)$ [16, 82–84]. After some algebra, we find that Eve's conditional covariance matrix is given by

$$\mathbf{V}_{eE'|b} = \begin{pmatrix} \mathbf{A} & \mathbf{D} \\ \mathbf{D}^T & \mathbf{C} \end{pmatrix}, \quad \text{(A21)}$$

with

$$\mathbf{A} = W\mathbf{I} - \frac{(1-T)(W^2-1)}{\theta}\mathbf{\Pi}, \quad \text{(A22)}$$

$$\mathbf{C} = \Lambda(W,V_A)\,\mathbf{I} - \frac{\alpha}{\theta}\mathbf{\Pi}, \quad \text{(A23)}$$

$$\mathbf{D} = \sqrt{T(W^2-1)}\mathbf{Z} - \frac{\gamma}{\theta}\mathbf{\Pi}, \quad \text{(A24)}$$

where we defined

$$\alpha = (1-T)\,T\left[W - V_a + V_0\right]^2, \quad \text{(A25)}$$

$$\theta := \Lambda(V_A, W) + \frac{1-\eta}{\eta}S, \quad \text{(A26)}$$

$$\gamma := (1-T)(W-V_A)\sqrt{T(W^2-1)}. \quad \text{(A27)}$$

We then compute the conditional symplectic spectrum. In the limit of large modulation ($V_a \gg 1$), we derive

$$\bar{\nu}_3 \to \sqrt{\frac{W\left[S(1-T)(1-\eta)+\eta\right]}{S(1-T)(1-\eta)+W\eta}}, \quad \text{(A28)}$$

$$\bar{\nu}_4 \to \sqrt{\frac{(1-T)\left[S(1-\eta)(1-T)+W\eta\right]}{T\eta}V_a}. \quad \text{(A29)}$$

These can be used to compute Eve's conditional entropy $H_c^{\blacktriangleleft}$. Therefore, we find

$$\chi(E:b) = H - H_c^{\blacktriangleleft}, \quad \text{(A30)}$$

$$\to h(W) - h(\bar{\nu}_3) + \frac{1}{2}\log_2\frac{(1-T)T\eta V_a}{S(1-\eta)(1-T)+W\eta}.$$

Finally, by using $I(a:b)$ previously computed, we can derive the asymptotic secret-key rate in RR

$$R^{\blacktriangleleft}(V_0,T,W,\eta,S) = h(\bar{\nu}_3) - h(W) + \frac{1}{2}\log\frac{(1-\eta)(1-T)S + W\eta}{(1-T)[\eta\Lambda(V_0,W)+(1-\eta)S]}. \quad \text{(A31)}$$

Appendix B: Coherent Bidirectional Terahertz-Optical Converter

The proposed converter consists of a terahertz cavity mode, an optical cavity mode, and a phononic mode treated in a linearized approximation. Introducing the vector of quadrature operators

$$\vec{x} = (q_o, q_t, q_m, p_o, p_t, p_{qp})^{\mathrm{T}}, \tag{B1}$$

the Hamiltonian, defined in a frame rotating with respect to the oscillator resonance frequencies, is $H = \vec{x}^T \mathbf{G}\vec{x}/2$ where $\mathbf{G} = \mathrm{Diag}(\mathbf{g}, \mathbf{g})$ with

$$\mathbf{g} = \begin{pmatrix} 0 & 0 & g_o \\ 0 & 0 & g_t \\ g_o & g_t & 0 \end{pmatrix}. \tag{B2}$$

The Heisenberg-Langevin equations corresponding to this Hamiltonian are

$$\dot{\vec{x}} = \mathbf{M}\,\vec{x} + \mathbf{N}\,\vec{x}_{\mathrm{in}}, \tag{B3}$$

with the input noise operators are defined in the usual way [79] and the matrices as

$$\mathbf{M} = \begin{pmatrix} -\mathbf{n}^2/2 & \mathbf{g} \\ -\mathbf{g} & -\mathbf{n}^2/2 \end{pmatrix}, \tag{B4a}$$

$$\mathbf{N} = \mathrm{Diag}(\mathbf{n}, \mathbf{n}), \tag{B4b}$$

where $\mathbf{n} = \mathrm{Diag}(\sqrt{\kappa_o}, \sqrt{\kappa_t}, \sqrt{\kappa_{qp}})$.

Taking the Fourier transform of Eq. (B3) and rearranging the resulting equation, we obtain the Fourier transform of the intracavity quadrature operators in terms of the input field quadrature operators as

$$(\mathbf{M} + i\omega\mathbf{1})\vec{x}(\omega) = -\mathbf{N}\,\vec{x}_{in}(\omega). \tag{B5}$$

Substituting the standard input-output boundary condition [79], in the form

$$\vec{x}_{in}(\omega) + \vec{x}_{out}(\omega) = \mathbf{N}\,\vec{x}(\omega), \tag{B6}$$

into Eq. (B5), and again rearranging, we obtain the output fields in terms of the input fields as

$$\vec{x}_{out}(\omega) = -\left[\mathbf{N}(\mathbf{M} + i\omega\mathbf{1})^{-1}\mathbf{N} + \mathbf{1}\right]\,\vec{x}_{in}(\omega). \tag{B7}$$

Taking the expectation values of this equation, we obtain

$$\langle\vec{x}_{out}(\omega)\rangle = \mathbf{H}(\omega)\langle\vec{x}_{in}(\omega)\rangle, \tag{B8}$$

where $\mathbf{H}(\omega)$ is the matrix of frequency responses,

$$\mathbf{H}(\omega) = -\mathbf{N}(\mathbf{M} + i\omega\mathbf{1})^{-1}\mathbf{N} - \mathbf{1}. \tag{B9}$$

Assuming that the outputs and inputs are initially in the vacuum state, this matrix of frequency responses enables a complete description of the input-output behavior of the converter.

Now we are interested in the elements of $\mathbf{H}(\omega)$ relating an input terahertz quadrature to an output optical quadrature, or an input optical quadrature to an output terahertz quadrature. It turns out that the nonzero frequency responses relate either input and output q quadratures, or input and output p quadratures. In fact, the form of the frequency responses are independent of whether we are considering q or p quadratures. So henceforth we focus exclusively on the q quadratures, with the understanding that the same results apply to the p quadratures.

Next, the q quadrature terahertz-to-optical frequency response and optical-to-terahertz frequency response are given by the matrix elements

$$H_{12}(\omega) = \frac{\langle\hat{q}_{\mathrm{o,out}}(\omega)\rangle}{\langle\hat{q}_{\mathrm{t,in}}(\omega)\rangle},\ H_{21}(\omega) = \frac{\langle\hat{q}_{\mathrm{t,out}}(\omega)\rangle}{\langle\hat{q}_{\mathrm{o,in}}(\omega)\rangle}, \tag{B10}$$

respectively. It turns out that, aside from the differing reference frames which have been transformed out of this description, the terahertz-to-optical frequency response is the same as the optical-to-terahertz frequency response. Therefore, we may define a single frequency-dependent transmissivity, as indicated in Eq. (20) of the main text, by

$$t(\omega) \equiv H_{12}(\omega) = H_{21}(\omega), \tag{B11}$$

Now using Eq. (B9), we find that

$$t(\omega) = \frac{-8g_{\mathrm{o}}g_{\mathrm{t}}\sqrt{\kappa_{\mathrm{o}}\kappa_{\mathrm{t}}}}{4g_{\mathrm{t}}^2(\kappa_{\mathrm{o}} - 2i\omega) + (\kappa_{\mathrm{t}} - 2i\omega)d(\omega)}, \tag{B12a}$$

$$d(\omega) = 4g_{\mathrm{o}}^2 + (\kappa_{\mathrm{o}} - 2i\omega)(\kappa_{\mathrm{qp}} - 2i\omega). \tag{B12b}$$

Setting $\omega = 0$, corresponding to a terahertz signal at ω_t and an optical signal at ω_o, then leads to the zero-frequency gain quoted in Eq. (21) of the main text.

In the limit of negligible quasiparticle damping ($\kappa_{qp} \to 0$), symmetric couplings ($g_o = g_t = g$), and symmetric out-couplings ($\kappa_o = \kappa_t = \kappa$), we have $|t(\omega = 0)| \to 1$. The frequency-dependence of the magnitude and phase response may also be studied in this limit, in order to ascertain the useful bandwidth of the converter. They are given by

$$|t(\omega)|^2 = \frac{\kappa^2}{\kappa^2 + 4\omega^2}\frac{16g^4}{16g^2(g^2 - \omega^2) + \omega^2(\kappa^2 + 4\omega^2)}, \tag{B13a}$$

$$\phi(\omega) = \tan^{-1}\left[\frac{\omega(8g^2 + \kappa^2 - 4\omega^2)}{4\kappa(g^2 - \omega^2)}\right], \tag{B13b}$$

respectively. The group delay through the converter, $g(\omega) = d\phi/d\omega$, is obtained from Eq. (B13b) as

$$g(\omega) = \frac{2\kappa}{\kappa^2 + 4\omega^2} + \frac{2\kappa(2g^2 + \omega^2)}{16g^2(g^2 - \omega^2) + \omega^2(\kappa^2 + 4\omega^2)}. \tag{B14}$$

To determine the bandwidth across which the magnitude response and group delay are approximately constant, we

Taylor expand Eqs. (B13a) and (B14) in the (assumed) small parameters ω/κ and ω/g. This yields the approximations

$$|t(\omega)|^2 = 1 - \frac{(\kappa^2 - 8g^2)^2}{16g^4\kappa^2}\omega^2 + \mathcal{O}\left[(\omega/\kappa)^4, (\omega/g)^4\right], \tag{B15a}$$

$$g(\omega) = \frac{8g^2 + \kappa^2}{4g^2\kappa} + \left(\frac{3\kappa}{8g^4} - \frac{8}{\kappa^3} - \frac{\kappa^3}{64g^6}\right)\omega^2 + \mathcal{O}\left[(\omega/\kappa)^3, (\omega/g)^3\right]. \tag{B15b}$$

We would expect that $g \ll \kappa$ in the proposed device, and in this regime the quadratic terms in Eqs. (B15a) and (B15b) are negligible provided that

$$\omega \ll 4g(g/\kappa), \tag{B16}$$

in addition to the assumed regime, $\omega \ll g, \kappa$. If we assume $g = 10^8\,\mathrm{s}^{-1}$ and $\kappa = 10^9\,\mathrm{s}^{-1}$, then the bandwidth over which we would expect high-fidelity transmission is of the order of $\sim 10\,\mathrm{MHz}$.

[1] C. E. Shannon, Bell Syst. Tech. J. **27**, 623 (1948).
[2] J. F. Federici, L. Moeller, and K. Su, *Terahertz Communication*, in Handbook of terahertz technology for imaging and sensing, D. Saeedkia, Editor, (Woodhead Publishing Cambridge, 2013).
[3] J. F. Federici and L. Moeller, Journal of Applied Physics **107**, 111101 (2010)..
[4] I. F. Akyildiz, J.M. Jornet, and C. Han, Physical Communication **12**, 16 (2014).
[5] I. F. Akyildiz, J. M. Jornet, and C. Han, IEEE Wireless Communications **21**, 130 (2014).
[6] T. Nagatsuma, S. Horiguchi, Y. Minamikata, Y. Yoshimizu, S. Hisatake, S. Kuwano, N. Yoshimoto, J. Terada, and H. Takahashi, Optics Express **21**, 23736 (2013).
[7] T. Kleine-Ostmann and T. Nagatsuma, J. Infrared, Millimeter, and THz Waves **32**, 143 (2011).
[8] T. Schneider, A. Wiatrek, S. Preußler, M. Grigat, and R.-P. Braun, IEEE Transactions on terahertz science and technology **2**, 250 (2012).
[9] J. Ma, F. Vorrius, L. Lamb, L. Moeller, and J. F. Federici, Journal of Infrared, Millimeter, and Terahertz Waves **36**, 1195 (2015).
[10] J. Ma, F. Vorrius, L. Lamb, L. Moeller, and J. F. Federici, Journal of Infrared, Millimeter, and Terahertz Waves **36**, 856 (2015).
[11] J. Ma, L. Moeller, and J. F. Federici, Journal of Infrared, Millimeter, and Terahertz Waves **36**, 130 (2015).
[12] K. Su, L. Moeller, R. B. Barat, and J. F. Federici, J. Opt. Soc. Am. A **29**, 2360 (2012).
[13] K. Su, L. Moeller, R. B. Barat, and J. F. Federici, J. Opt. Soc. Am. A **29**, 179 (2012).
[14] J. Sun, F. Hu, and S. Lucyszyn, IEEE Access **4** 9377 (2016).
[15] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lutkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).
[16] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, Rev. Mod. Phys. **84**, 621 (2012).
[17] J. Watrous, *The theory of quantum information* (Cambridge University Press, Cambridge, 2018). Also available from https://cs.uwaterloo.ca/~watrous/TQI/TQI.pdf
[18] M. Hayashi, *Quantum Information Theory: Mathematical Foundation* (Springer-Verlag Berlin Heidelberg, 2017).
[19] V. Scarani, S. Iblisdir, N. Gisin, and A. Acin, Rev. Mod. Phys. **77**, 1225 (2005).
[20] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Rev. Mod. Phys. **81**, 865 (2009).
[21] S. L. Braunstein, and P. van Loock, Rev. Mod. Phys. **77**, 513 (2005).
[22] E. Diamanti, and A. Leverrier, Entropy **17**, 6072 (2015).
[23] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Nat. Commun. **8**, 15043 (2017); See also arXiv:1510.08863 and arXiv:1512.04.
[24] S. Pirandola, S. L. Braunstein, R. Laurenza, C. Ottaviani, T. P. W. Cope, G. Spedalieri, and L. Banchi, arXiv:1711.09909.
[25] C. Ottaviani, R. Laurenza, T. P. W. Cope, G. Spedalieri, S. L. Braunstein, and S. Pirandola, Proc. SPIE **9996**, 999609 (2016).
[26] F. Grosshans, and P. Grangier, Phys. Rev. Lett. **88**, 057902 (2002).
[27] F. Grosshans *et al.*, Nature **421**, 238-241 (2003).
[28] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, P. K. Lam, Phys. Rev. Lett. **93**, 170504 (2004).
[29] V. C. Usenko, and F. Grosshans, Phys. Rev. A **92**, 062337 (2015).
[30] S. Pirandola, S. Mancini, S. Lloyd, and S. L. Braunstein, Nat. Phys. 4, **726** (2008).
[31] C. Ottaviani, S. Mancini, and S. Pirandola, Phys. Rev. A **92**, 062323 (2015).
[32] M. Sun, X. Peng, Y. Shen, and H. Guo, Int. J. Quantum Inform. **10**, 1250059 (2012).
[33] Y. -C. Zhang, Z. Li, C. Weedbrook, S. Yu, W. Gu, M. Sun, X. Peng, H. Guo, J. Phys. B **47**, 035501 (2014).
[34] S. Pirandola *et al.*, Nat. Phot. **9**, 397 (2015).
[35] C. Weedbrook, Phys. Rev. A **87**, 022308 (2013).
[36] J. Lodewyck, et al. Phys. Rev. A **76**, 042305 (2007).
[37] C. Weedbrook, S. Pirandola, S. Lloyd, and T. C. Ralph, Phys. Rev. Lett. **105**, 110501 (2010).
[38] C. Weedbrook, S. Pirandola, and T. C. Ralph, Phys. Rev. A **86**, 022318 (2012).
[39] C. Weedbrook, C. Ottaviani, and S. Pirandola, Phys. Rev. A **89**, 12309 (2014).
[40] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, Nat. Phot. **7**, 378 (2013).
[41] T. Gehring, C. S. Jacobsen, and U. L. Andersen, Quant. Inf. Comput. **16**, 1081 (2016).
[42] S Pirandola *et al.*, Nat. Phot. **9**, 773 (2016).
[43] D. Huang, P. Huang, D. Lin, and G. Zeng, Sci. Rep. **6,** 19201 (2016).

[44] J. Fiurà̀šek, and N. J. Cerf, Phys. Rev. A **86**, 060302(R) (2012).

[45] N. Walk, T. Symul, P. K. Lam, T. C. Ralph, Phys. Rev. A. **87**, 020303, (2013).

[46] R. Blandino, A. Leverrier, M. Barbieri, J. Etesse, P. Grangier, and R. Tualle-Brouri, Phys. Rev. A **86**, 012327 (2012).

[47] M. Milicevic, C. Feng, L. M. Zhang, and P. Glenn Gulak, npj Quantum Information **4**, 21 (2018).

[48] X. Wang, Y.-C. Zhang, Z. Li, B. Xu, S. Yu, and H. Guo, Quant. Inf. Comput. **17**, 1123 (2017).

[49] P. Papanastasiou, C. Ottaviani, and S. Pirandola, arXiv:1803.09158 (2018).

[50] M. Navascués, F. Grosshans, and A. Acín, Phys. Rev. Lett. **97**, 190502 (2006).

[51] R. García-Patrón, and N. J. Cerf, Phys. Rev. Lett. **97**, 190503 (2006).

[52] S. Pirandola, S. L. Braunstein, and S. Lloyd, Phys. Rev. Lett. **101**, 200504 (2008).

[53] A. Leverrier, Phys. Rev. Lett. **118**, 200501 (2017).

[54] R. Renner, N. Gisin, and B. Kraus, Phys. Rev. A **72**, 012332 (2005).

[55] R. Renner, and J. I. Cirac, Phys. Rev. Lett. **102**, 110504 (2009).

[56] C. Ottaviani, S. Mancini, and S. Pirandola, Phys. Rev. A **95**, 052310 (2017).

[57] C. Ottaviani, and S. Pirandola, Sci. Rep. **6**, 22225 (2016).

[58] R. W. Andrews *et al.*, Nat. Phys. **10**, 321 (2014).

[59] Q. Zhang *et al.*, Nat. Phys. **12**, 1005 (2016).

[60] J. Kerckhoff *et al.*, Phys. Rev. X **3**, 021013 (2013).

[61] C. Belacel, Y. Todorov, S. Barbieri, D. Gacemi, I. Favero, and C. Sirtori, Nat. Comm. **8,** 1578 (2017).

[62] F. Grosshans, N. J. Cerf, J. Wenger, R. Tualle-Brouri, and P. Grangier, Quant. Inf. Comput. **3**, 535 (2003).

[63] S. Lloyd, Science **321**, 1463 (2008).

[64] S.-H. Tan, B. I. Erkmen, V. Giovannetti, S. Guha, S. Lloyd, L. Maccone, S. Pirandola, and J. H. Shapiro, Phys. Rev. Lett. **101**, 253601 (2008).

[65] J. H. Shapiro, and S. Lloyd, New J. Phys. **11**, 063045 (2009).

[66] S. Barzanjeh, S. Guha, C. Weedbrook, D. Vitali, J. H. Shapiro, and S. Pirandola, Phys. Rev. Lett. **114**, 080503 (2015).

[67] C. Weedbrook, S. Pirandola, J. Thompson, V. Vedral, and M. Gu, New J. Phys. **18,** 043027 (2016).

[68] J. H. Shapiro, Phys. Rev. A **80**, 022320 (2009).

[69] Z. Zhang, M. Tengner, T. Zhong, F. N.C. Wong, and J. H. Shapiro, Phys. Rev. Lett. **111**, 010501 (2013).

[70] A. S. Holevo, Probl. Inf. Transm. **9**, 177-183 (1973).

[71] A. S. Holevo, M. Sohma, and O. Hirota, Phys. Rev. A **59**, 1820-1828 (1999).

[72] H. Yonezawa, S.L. Braunstein, and A. Furusawa, Phys. Rev. Lett. **99**, 110503 (2007).

[73] S. Yokoyama *et al.*, Nat. Phot. **7**, 982 (2013).

[74] J. Bochmann, A. Vainsencher, D. D. Awschalom, and A. N. Cleland, Nat. Phys. **9**, 712 (2013).

[75] T. Bagci *et al.*, Nature **507**, 81 (2014).

[76] H. J. Kimble, Nature **453**, 1023 (2008).

[77] S. Pirandola, and S. L. Braunstein, Nature **532**, 169 (2016).

[78] S. Pirandola, J. Eisert, C. Weedbrook, A. Furusawa, and S. L. Braunstein, Nat. Phot. **9**, 641-652 (2015).

[79] C. W. Gardiner, and P. Zoller, *Quantum Noise* (Springer Berlin Heidelberg, 2004).

[80] R. Kakimi, M. Fujita, M. Nagai, M. Ashida, and T. Nagatsuma, Nat. Phot. **8**, 657 (2014).

[81] M. Eichenfield, J. Chan, R. M. Camacho, K. J. Vahala, O. Painter, Nature **462**, 78 (2009).

[82] J. Eisert, S. Scheel, and M. B. Plenio, Phys. Rev. Lett. **89**, 137903 (2002).

[83] J. Fiurà̀šek, Phys. Rev. Lett. **89**, 137904 (2002).

[84] G. Spedalieri, C. Ottaviani, and S. Pirandola, Open Syst. Inf. Dyn. **20**, 1350011 (2013).