Here, we present the detailed models and experimental parameters that we use for the numerical simulations shown in Fig. 1 of the main text. Also, we briefly discuss challenges associated with the state preparation process in CV-MDI-QKD.

I. DV-MDI-QKD

The secure key rate of decoy-state DV-MDI-QKD in the asymptotic limit of an infinitely long key is given by [1]

\[ R_{DV} = p_{11}^Z Y_{11}^Z [1 - H_2(c_{11}^X)] - Q^Z f_e(E^Z) H_2(E^Z), \] (1)

where \( p_{11}^Z = \mu_A \mu_B e^{-((\mu_A + \mu_B)\lambda)} \) denotes the joint probability that both Alice and Bob generate a single-photon pulse, and with \( \mu_A \) and \( \mu_B \) being, respectively, the intensity of Alice and Bob’s signal states; the parameters \( Y_{11}^Z \) and \( c_{11}^X \) are, respectively, the yield in the rectilinear (Z) basis and the error rate in the diagonal (X) basis, given that both Alice and Bob send single-photon states; \( H_2(x) = -x \log_2(x) - (1 - x) \log_2(1 - x) \) is the binary Shannon entropy function; the terms \( Q^Z \) and \( E^Z \) denote, respectively, the overall gain and quantum bit error rate (QBER) in the Z basis when both Alice and Bob emit a single photon; and \( f_e(E^Z) \geq 1 \) is the error correction inefficiency function.

The quantities \( Q^X \) and \( E^X \) are directly measured in the experiment, while \( Y_{11}^Z \) and \( c_{11}^X \) can be estimated using the decoy-state method [2]. Importantly, it has been shown that the use of two decoy states is enough to obtain a tight estimation for \( Y_{11}^Z \) and \( c_{11}^X \) [3].

To model experimental errors, we employ the method proposed in ref. [2] for polarization encoding DV-MDI-QKD [4, 5]. See also refs. [6, 7] for alternative models suitable for time-bin encoding systems [8, 9]. In particular, we use two unitary operators, located at the input arms of the beamsplitter within the relay (see Appendix B in ref. [2]), to simulate the intrinsic error rate, denoted as \( e_d \), due to the misalignment and instability of the optical system. In addition, we consider threshold single-photon detectors (SPDs) with detection efficiency \( \eta_d \) and dark count rate \( Y_0 \). Furthermore, for simplicity, we consider the asymptotic case where Alice and Bob use an infinite number of decoy states. As already mentioned, the practical situation with a finite number of decay settings provides similar results [3]. In this scenario, we have that the parameters \( Y_{11}^Z \) and \( e_{11}^X \) have the form [2]

\[
Y_{11}^Z = (1 - Y_0)^2 \left[ 4Y_0^2 (1 - \eta_A \eta_d)(1 - \eta_B \eta_d) + 2Y_0 \left( \eta_A \eta_d + \eta_B \eta_d - \frac{3}{2} \eta_A \eta_B \eta_d^2 \right) + \frac{1}{2} \eta_A \eta_B \eta_d^2 \right],
\]

\[
e_{11}^X = \frac{1}{2} - \frac{(1 - Y_0)^2 \eta_A \eta_B \eta_d^2 (1 - e_d)^2}{4Y_0^2 Y_{11}^Z},
\] (2)

where \( \eta_A \) (\( \eta_B \)) denotes the channel transmittance from Alice (Bob) to the relay. That is, \( \eta_A = 10^{-\alpha l_A/10} \), where \( \alpha \) is the loss coefficient of the channel that connects Alice with the relay measured in dB/km, and \( l_A \) is the length of this channel measured in km. The definition of \( \eta_B \) is analogous. Moreover, we have that \( Y_{11}^X = Y_{11}^Z \).

For simulation purposes only, we use the value of \( Q^X \) and \( E^X \) provided in Appendix B of ref. [2]. For completeness, we include the mathematical expressions below. In particular,

\[ Q^X = \frac{1}{2} \left( \Omega_1 + \Omega_2 \right), \]

\[ E^X = \frac{\Omega_1}{\Omega_1 + \Omega_2}, \] (3)

where the parameters \( \Omega_1 \) and \( \Omega_2 \) are given by

\[ \Omega_1 = 2e^{-\frac{x}{2}} (1 - Y_0)^2 \left[ I_0(\beta) + I_0(\beta - 2\beta e_d) \right] \]

\[ + 2(1 - Y_0)^2 e^{-\frac{x}{2}} - 2(1 - Y_0)e^{-\frac{(1 - e_d)\beta}{2}} I_0(e_d \beta) \]

\[ - 2(1 - Y_0)e^{-\frac{x}{2}} I_0(\beta - e_d \beta) \],

\[ \Omega_2 = 2e^{-\frac{x}{2}} (1 - Y_0)^2 \left[ 1 + I_0(2\lambda) + 2(1 - Y_0)^2 e^{-\frac{x}{2}} \right] \]

\[ - 2(1 - Y_0)e^{-\frac{x}{2}} I_0(\lambda) - 2(1 - Y_0)e^{-\frac{x}{2}} I_0(\lambda) \],

with \( I_0(x) \) being the modified Bessel function, and where

\[ \gamma = (\mu_A \eta_A + \mu_B \eta_B) \eta_d, \]

\[ \beta = \eta_d \sqrt{\mu_A \mu_B \eta_A \eta_B}, \]

\[ \lambda = \beta (1 - e_d), \]

\[ \omega = \mu_A \eta_A \eta_d + e_d (\mu_B \eta_B - \mu_A \eta_A) \eta_d. \] (5)
TABLE I: Experimental parameters considered in DV-MDI-QKD.

<table>
<thead>
<tr>
<th>$\eta_d$</th>
<th>$e_d$</th>
<th>$Y_0$</th>
<th>$I_{a}(E^2)$</th>
</tr>
</thead>
</table>

In our simulation, we employ the experimental parameters shown in Table I. That is, we consider high-efficiency WSi superconducting nanowire single-photon detectors (SNSPDs) with $\eta_d = 93\%$ and $Y_0 = 10^{-6}$ (per pulse) [10], and assume an intrinsic error rate $e_d = 0.1\%$ (which corresponds to the QBER of 0.25\% obtained in the 200 km DV-MDI-QKD experiment reported in ref. [11]). In addition, we use $I_{a}(E^2) = 1.16$ [12]. The resulting lower bound on the secret key rate $R_{DV}$ given by Eq. (1) is illustrated in Fig. 1 in the main text, where we have numerically optimised the values of the intensities $\mu_A$ and $\mu_B$. That is, for a given total system loss, we use a Monte Carlo simulation method to select the value of $\mu_A$ and $\mu_B$ such that $R_{DV}$ is maximum.

To conclude this section, let us emphasise that the high-dimensional QKD [13, 14] and a proof-of-principle demonstration of DV-MDI-QKD [15].

II. CV-MDI-QKD

To evaluate the secure key rate of CV-MDI-QKD we follow Section E from the Supplementary Information of ref. [16]. We have that the general expression of the key rate formula has the form

$$R_{CV} = \xi I_{AB} - I_E,$$  

(6)

where $\xi$ is the reconciliation efficiency of the error correction code, and $I_{AB}$ and $I_E$ denote, respectively, Alice and Bob’s mutual information and Eve’s stolen information on Alice’s key.

To derive an explicit formula for the secret key rate given by Eq. (6), Pirandola et al. [16] consider a “realistic Gaussian attack against the two links”, which definitively provides an upper bound on the secure key rate. Here, we assume the most favourable situation for CV-MDI-QKD by considering that such realistic Gaussian attack is indeed optimal and the resulting key rate is achievable. In doing so, we have that the quantity $I_{AB}$ can be expressed as [16]

$$I_{AB} = \log_2 \left( \frac{\phi + 1}{\chi} \right),$$  

(7)

where $\phi$ is the modulation variance in shot-noise units and $\chi$ represents the so-called equivalent noise.

Moreover, for simplicity, we consider the key rate in the limit of large modulation ($\phi \gg 1$). In this scenario, and considering first the asymmetric case $\eta_A \neq \eta_B$, we have that $I_E$ is given by [16]

$$I_E = h(\beta) + \log_2(\gamma) - h(\delta),$$  

(8)

where the parameters $\beta$, $\gamma$ and $\delta$ have the form

$$\beta = \frac{\eta_A \eta_B \chi - (\eta_A + \eta_B)^2}{\eta_A - \eta_B (\eta_A + \eta_B)},$$

$$\gamma = \frac{e(\eta_A - \eta_B (\phi + 1))}{2(\eta_A + \eta_B)},$$

$$\delta = \frac{\eta_A \chi - (\eta_A + \eta_B)}{\eta_A + \eta_B}.$$  

(9)

Here, the term $e$ denotes Euler’s number, and the equivalent noise $\chi$ is given by

$$\chi = \frac{2(\eta_A + \eta_B)}{\eta_A\eta_B\eta_d} + \varepsilon,$$  

(10)

with $\varepsilon$ being the excess noise. Finally, the function $h(x)$, which appears in Eq. (8), has the form

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

In the symmetric case where $\eta_A = \eta_B = \eta$, we have that $I_E$ is given by [16]

$$I_E = \log_2 \left( \frac{e(\chi - 4) (\phi + 1)}{16} \right) - h \left( \frac{\chi - 1}{2} \right),$$  

(11)

where the equivalent noise $\chi$ has now the form

$$\chi = \frac{4}{\eta_d} + \varepsilon.$$  

(12)

In the simulation shown in Fig. 1 in the main text, we consider the same experimental parameters used in ref. [16]. They are illustrated in Table II.

TABLE II: Experimental parameters considered in CV-MDI-QKD [16].

<table>
<thead>
<tr>
<th>$\eta_d$</th>
<th>$\varepsilon$</th>
<th>$\phi$</th>
<th>$\xi$</th>
</tr>
</thead>
<tbody>
<tr>
<td>98%</td>
<td>0.01</td>
<td>60</td>
<td>0.97</td>
</tr>
</tbody>
</table>

III. TGM BOUND

The secret key rates obtained in the previous sections can be compared with the fundamental upper bound (per optical mode) for coherent-state QKD provided in ref. [17] (so-called TGW bound). This bound has the form

$$R_{TGW} = \log_2 \left( \frac{1 + \eta_A \eta_B}{1 - \eta_A \eta_B} \right).$$  

(13)

It can be shown, for instance, that at a typical metropolitan distance (say 20 km of standard telecom fiber of loss 0.2 dB/km used as an example in [16]), the key rate of DV-MDI-QKD is approximately two orders of magnitude away from this fundamental limit.
IV. SOURCE REQUIREMENTS IN CV-MDI-QKD

As already mentioned in the main text, the experimental configuration using one laser feeding two closely spaced Alice and Bob on the optical table bypasses one of the major experimental challenges in CV-MDI-QKD, namely, establishing a reliable phase reference between two remote users. Even if a common laser is used for both Alice and Bob, distributing phase-stable signals over fibre to two remote sites can still be a practical challenge.

Furthermore, it is important to emphasize that one fundamental assumption in MDI-QKD is that Eve cannot interfere with Alice and Bob’s state preparation processes [1]. To justify the above assumption, DV-MDI-QKD is commonly implemented by using independent laser sources for Alice and Bob. However, since the proof-of-principle demonstration in ref. [16] uses a common laser source for both of them, this might open the door for side-channel attacks on quantum state preparation. This is because at least one of the users has to encode information on untrusted laser pulses accessible by Eve.

Pirandola et al. [16] discussed several potential solutions to the above problems in the Supplementary Information. However, none of them has been implemented in ref. [16].

Acknowledgements: The authors thank Z.-Y. Li and J. Shapiro for valuable discussions. Support from the Office of Naval Research (ONR), the Air Force Office of Scientific Research (AFOSR), the Galician Regional Government (program “Ayudas para proyectos de investigación desarrollados por investigadores emergentes”), and consolidation of Research Units: AtlantTIC), the Spanish Ministry of Economy and Competitiveness (MINECO), the “Fondo Europeo de Desarrollo Regional” (FEDER) through grant TEC2014-54898-R, NSERC, CFI, and ORF is gratefully acknowledged.

* Electronic address: fhxu@mit.edu