Supplementary Information: Gigahertz measurement-device-independent quantum key distribution using directly modulated lasers

R. I. Woodward[1,2,*], Y. S. Lo[1,3], M. Pittaluga[1,4], M. Minder[1,5], T. K. Paraïso[1], M. Lucamarini[1], Z. L. Yuan[1], A. J. Shields[1]
[1] *Toshiba Europe Ltd, Cambridge, UK*
[2] *Quantum Communications Hub, University of York, UK*
[3] *Quantum Science and Technology Institute, University College London, UK*
[4] *School of Electronic and Electrical Engineering, University of Leeds, UK*
[5] *Department of Engineering, University of Cambridge, UK* *
(Dated: March 3, 2021)

CONTENTS

SUPPLEMENTARY NOTE 1: PHASE RANDOMISATION

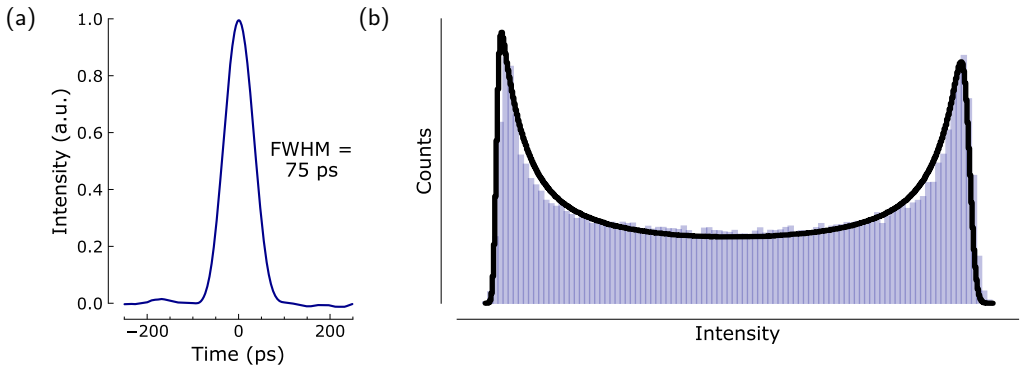
To satisfy the security proofs of decoy-state MDI-QKD it is important that phase is randomised between weak coherent states. Our setup intrinsically achieves this by the nature of gain-switching the primary laser: by periodically driving the laser below threshold each clock cycle for a sufficient time for the laser cavity to empty of photons, each pulse grows from spontaneous emission—i.e. is effectively seeded by random vacuum fluctuations.

This is confirmed by passing the unattenuated pulse train (where each pulse has 75 ps duration, as shown in Supplementary Fig. 1a) from each transmitter through an asymmetric Mach-Zehnder interferometer (AMZI) with one arm delayed to interfere consecutive coherent states. The output intensity is measured on a photodiode and oscilloscope, then processed to form a histogram of the output intensities at the centre of 10^5 pulses. The histogram (Supplementary Fig. 1b) exhibits the $1 + \cos(\phi)$ shape expected for interference of pulses with uniformly distributed random relative phase ϕ, including accounting for experimental uncertainties [1].

SUPPLEMENTARY NOTE 2: FOUR-INTENSITY DECOY STATE PROTOCOL & KEY RATE CALCULATION

We employ a 4-intensity decoy-state protocol [2] for MDI-QKD, described as follows. Alice and Bob prepare weak coherent states with fluxes μ_i and μ_j, respectively, encoded with a random bit value $\{0, 1\}$. Pulses prepared in the Z-basis are signal states with flux $\mu = s$, which are used to generate secure key material, whereas states in the X-basis can be $\mu \in \{u, v, w\}$, corresponding to 3 possible decoy states that are used for parameter estimation to bound the single-photon yield and error rate. States are prepared randomly with selection probability $P \in \{P_Z^s, P_X^u, P_X^v, P_X^w\}$, where the probability of encoding in the Z-basis is $P_Z = P_Z^s$ and in the X-basis is $P_X = P_X^u + P_X^v + P_X^w$, such that $P_Z + P_X = 1$.

* robert.woodward@crl.toshiba.co.uk



Supplementary Figure 1. Characterisation of transmitter output: (a) pulse shape measured on oscilloscope; (b) histogram of pulse amplitudes after AMZI (blue bars) and simulated AMZI output accounting for experimental imperfections (black line) showing that pulse phase is randomised.

To generate a secure key, Alice and Bob send their prepared states along the quantum communication channel to Charlie, who performs a Bell state measurement and announces which states resulted in a successful projection onto the singlet Bell state. Alice and Bob then engage in classical communication to share basis information and perform sifting, parameter estimation, error correction and privacy amplification. In practical communication, the finite sample size of states measured prior to processing means that all measurements are subject to statistical fluctuations, which thus need to be incorporated in the security analysis.

A proof-of-principle measurement is performed to highlight the secure key rate that is achievable from our gigahertz-clocked MDI-QKD system. The gain and QBER are measured for all possible combinations of weak coherent states, denoted $Q_{\Theta}^{\mu_i,\mu_j}$ and $E_{\Theta}^{\mu_i,\mu_j}$, respectively, for basis $\Theta \in \{X, Z\}$ and flux $\mu \in \{s, u, v, w\}$. These measurements are then used to estimate lower-bounded single-photon yield $\underline{y}_{\Theta}^{1,1}$ and upper-bounded error rate $\overline{e}_{\Theta}^{1,1}$, from which a lower bound of the secure key rate is computed as:

$$R = \underline{q}_{Z}^{1,1}\left[1 - h\left(\overline{e}_{X}^{1,1}\right)\right] - f_{EC}\; Q_{Z}^{s,s}\; h\left(E_{Z}^{s,s}\right) - \Delta. \tag{1}$$

where $\underline{q}_{Z}^{1,1} = \underline{y}_{Z}^{1,1}\left(P_Z\; s\; e^{-s}\right)^2$, $h(\cdot)$ is the binary entropy function, $f_{\mathrm{EC}} = 1.16$ accounts for error-correction inefficiency and Δ is a reduction due to finite size effects (discussed later).

We now summarise the relevant equations and our numerical approach for computing the single-photon yield and error bounds, in order to evaluate Eqn. 1. Full proofs can be found in Refs. [2–4] and a detailed derivation of the security analysis in Ref. [5].

A. Asymptotic Analysis

We begin with an asymptotic analysis that neglects finite-size effects, enabling our results to be compared to other works where statistical fluctuations are not considered. The first step is to find the single-photon yield and error rate in the X-basis, $\underline{y}_{X}^{1,1}$ and $\overline{e}_{X}^{1,1}$. While analytical equations have been derived to estimate these quantities [6], a more accurate value that takes all experimental constraints into account can be found by following a numerical approach. The gain of each weak coherent state combination is related to a summation over all possible photon number states that are emitted by Alice and Bob, accounting for Poisson photon statistics. By truncating this infinite summation, inequalities are formed which act as constraints for the numerical optimisation of $\underline{y}_{X}^{1,1}$, in addition to the logical requirement that $0 \leq y_{X}^{1,1} \leq 1$. Therefore, $\underline{y}_{X}^{1,1}$ can be estimated by the linear program:

$$\begin{aligned} &\text{minimise} \quad y_{X}^{1,1} \\ &\text{subject to} \quad 0 \leq y_{X}^{m,n} \leq 1, \\ &\qquad e^{-(\mu_i+\mu_j)} \sum_{m,n=0}^{S_{\mathrm{cut}}} \frac{\mu_i^m \mu_j^n}{m!n!} y_{X}^{m,n} \geq \max\left\{Q_{X}^{\mu_i,\mu_j} - \gamma_{ij}, 0\right\}, \\ &\qquad e^{-(\mu_i+\mu_j)} \sum_{m,n=0}^{S_{\mathrm{cut}}} \frac{\mu_i^m \mu_j^n}{m!n!} y_{X}^{m,n} \leq Q_{X}^{\mu_i,\mu_j}, \end{aligned} \tag{2}$$

where

$$\gamma_{ij} = e^{-(\mu_i+\mu_j)}\left[\left(\sum_{m=0}^{S_{\text{cut}}}\frac{\mu_i^m}{m!}\right)\left(e^{\mu_j}-\sum_{n=0}^{S_{\text{cut}}}\frac{\mu_j^n}{n!}\right)+\left(e^{\mu_i}-\sum_{m=0}^{S_{\text{cut}}}\frac{\mu_i^m}{m!}\right)\left(\sum_{n=0}^{S_{\text{cut}}}\frac{\mu_j^n}{n!}\right)+\left(e^{\mu_i}-\sum_{m=0}^{S_{\text{cut}}}\frac{\mu_i^m}{m!}\right)\left(e^{\mu_j}-\sum_{m=0}^{S_{\text{cut}}}\frac{\mu_j^n}{n!}\right)\right] \tag{3}$$

and the program is solved for all $n, m \leq S_{\text{cut}}$ ($S_{\text{cut}} = 15$ is an arbitrary integer that defines the maximum summation term) and $\mu_i, \mu_j \in \{u, v, w\}$. In practice, we solve the linear programming problems using the revised simplex method.

Following similar arguments, an additional linear program can be derived to estimate $\bar{e}_X^{1,1}$:

$$\begin{aligned}
&\text{maximise} && b_X^{1,1} \\
&\text{subject to} && 0 \leq b_X^{m,n} \leq 1, \\
&&& e^{-(\mu_i+\mu_j)}\sum_{m,n=0}^{S_{\text{cut}}}\frac{\mu_i^m\mu_j^n}{m!n!}b_X^{m,n} \geq \max\left\{B_X^{\mu_i,\mu_j}-\gamma_{ij},0\right\}, \\
&&& e^{-(\mu_i+\mu_j)}\sum_{m,n=0}^{S_{\text{cut}}}\frac{\mu_i^m\mu_j^n}{m!n!}y_X^{m,n}e_X^{m,n} \leq B_X^{\mu_i,\mu_j},
\end{aligned} \tag{4}$$

where bit error rate (BER) $B_X^{\mu_i,\mu_j} = Q_X^{\mu_i,\mu_j}E_X^{\mu_i,\mu_j}$ and $b_X^{m,n} = y_X^{m,n}e_X^{m,n}$. The single-photon error rate is extracted from the numerical solution by: $\bar{e}_X^{1,1} = \bar{b}_X^{1,1}/\underline{y}_X^{1,1}$. Finally, we note that in the asymptotic limit, $\underline{y}_Z^{1,1} = \underline{y}_X^{1,1}$ and $\Delta = 0$, enabling these numerically optimised terms to be inserted into Eqn. 1 to estimate the secure key rate.

B. Finite-Size Analysis

We now advance our analysis to account for statistical fluctuations in the data sample, starting with a widely used assumption that the fluctuations follow a Gaussian distribution [3]. A fluctuation function is defined: $F(\zeta, n) = n/\sqrt{\zeta}$ where n is the number of standard deviations which are summed over to quantify the statistical error in each measured value [3] (here, we use $n = 7$ to limit the failure probability to $< 10^{-10}$ [5]). Using this function, the linear programming problems to find $\underline{y}_X^{1,1}$ and $\bar{e}_X^{1,1}$ in the finite-size regime can be written as:

$$\begin{aligned}
&\text{minimise} && y_X^{1,1} \\
&\text{subject to} && 0 \leq y_X^{m,n} \leq 1, \\
&&& e^{-(\mu_i+\mu_j)}\sum_{m,n=0}^{S_{\text{cut}}}\frac{\mu_i^m\mu_j^n}{m!n!}y_X^{m,n} \geq \max\left\{Q_X^{\mu_i,\mu_j}\left[1-F(N_X^{\mu_i,\mu_j}Q_X^{\mu_i,\mu_j},7)\right]-\gamma_{ij},0\right\}, \\
&&& e^{-(\mu_i+\mu_j)}\sum_{m,n=0}^{S_{\text{cut}}}\frac{\mu_i^m\mu_j^n}{m!n!}y_X^{m,n} \leq \min\left\{Q_X^{\mu_i,\mu_j}\left[1+F(N_X^{\mu_i,\mu_j}Q_X^{\mu_i,\mu_j},7)\right],1\right\},
\end{aligned} \tag{5}$$

and

$$\begin{aligned}
&\text{maximise} && b_X^{1,1} \\
&\text{subject to} && 0 \leq b_X^{m,n} \leq 1, \\
&&& e^{-(\mu_i+\mu_j)}\sum_{m,n=0}^{S_{\text{cut}}}\frac{\mu_i^m\mu_j^n}{m!n!}b_X^{m,n} \geq \max\left\{Q_X^{\mu_i,\mu_j}\left[1-F(N_X^{\mu_i,\mu_j}B_X^{\mu_i,\mu_j},7)\right]-\gamma_{ij},0\right\}, \\
&&& e^{-(\mu_i+\mu_j)}\sum_{m,n=0}^{S_{\text{cut}}}\frac{\mu_i^m\mu_j^n}{m!n!}b_X^{m,n} \leq \min\left\{Q_X^{\mu_i,\mu_j}\left[1+F(N_X^{\mu_i,\mu_j}B_X^{\mu_i,\mu_j},7)\right],1\right\},
\end{aligned} \tag{6}$$

where $N_X^{\mu_i,\mu_j}$ is the number of states sent in the finite sample in the X-basis with fluxes μ_i and μ_j. Finally, the finite-size Z-basis single-photon yield is found as: $\underline{y}_Z^{1,1} = \underline{y}_X^{1,1} - \theta$ where θ takes into account possible fluctuations converting from $\underline{y}_X^{1,1}$ to $\underline{y}_Z^{1,1}$ and is fixed as 1.5×10^{-6} [5]. These single-photon quantities can then be inserted into Eqn. 1 to obtain the secure key rate.

C. Finite-Size Analysis with Composable Security

Finally, we discuss a more advanced finite-size analysis that relaxes assumption about the distribution of noise fluctuations and guarantees composable security against even coherent eavesdropper attacks [4, 5]. This is based on applying the multiplicative Chernoff bound to quantities in the measurement sample.

We start by bounding the number of states transmitted by the users $N_\Theta^{\mu_i,\mu_j}$, for each basis (Θ) and photon flux (μ_i, μ_j) combination. These quantities are disclosed during classical communication after the whole sample is measured, but due to the users' independent choices of basis and intensity, they are fluctuating quantities that must be bounded in the finite-size regime. By defining the function $g(x,y) = \sqrt{x\ln(y^{-2})}$, we can express the bounds such that $\overline{N}_\Theta^{\mu_i,\mu_j}$ ($\underline{N}_\Theta^{\mu_i,\mu_j}$) is guaranteed to be greater (smaller) than $N_\Theta^{\mu_i,\mu_j}$ with probability $1-\epsilon_0$:

$$\overline{N}_\Theta^{\mu_i\mu_j} = N_\Theta^{\mu_i\mu_j} + g(N_\Theta^{\mu_i\mu_j}, \epsilon_0^2) \tag{7}$$

$$\underline{N}_\Theta^{\mu_i\mu_j} = N_\Theta^{\mu_i\mu_j} - g(N_\Theta^{\mu_i\mu_j}, \epsilon_0^4). \tag{8}$$

where $\epsilon_0 = 4\times10^{-13}$ is used to limit the total failure probability to $< 10^{-10}$.

We can then follow a similar procedure to bound the number of successful Bell state measurement counts, $C_\Theta^{\mu_i\mu_j}$, and number of erroneous Bell state counts, $EC_X^{\mu_i\mu_j}$. (The quantities $C_\Theta^{\mu_i\mu_j}$ and $EC_\Theta^{\mu_i\mu_j}$ were directly measured in our experiment, however, they have been processed for displaying in Tables II & III as the gain and QBER by normalising them to to the number of transmitted states: $Q_\Theta^{\mu_i\mu_j} = C_\Theta^{\mu_i\mu_j}/N_\Theta^{\mu_i\mu_j}$ and $E_\Theta^{\mu_i\mu_j} = EC_\Theta^{\mu_i,\mu_j}/C_\Theta^{\mu_i,\mu_j}$). By replacing N in Eqns. 7–8 with C and EC, we find the bounds $\overline{C}_\Theta^{\mu_i\mu_j}$ & $\underline{C}_\Theta^{\mu_i\mu_j}$ and $\overline{EC}_\Theta^{\mu_i\mu_j}$ & $\underline{EC}_\Theta^{\mu_i\mu_j}$, respectively.

These bounded quantities can then be used to compute bounded gains and bit error rates:

$$\overline{Q}_\Theta^{\mu_i\mu_j} = \overline{C}_\Theta^{\mu_i\mu_j}/\underline{N}_\Theta^{\mu_i\mu_j} \tag{9}$$

$$\underline{Q}_\Theta^{\mu_i\mu_j} = \underline{C}_\Theta^{\mu_i\mu_j}/\overline{N}_\Theta^{\mu_i\mu_j} \tag{10}$$

$$\overline{B}_\Theta^{\mu_i\mu_j} = \overline{EC}_\Theta^{\mu_i\mu_j}/\underline{N}_\Theta^{\mu_i\mu_j} \tag{11}$$

$$\underline{B}_\Theta^{\mu_i\mu_j} = \underline{EC}_\Theta^{\mu_i\mu_j}/\overline{N}_\Theta^{\mu_i\mu_j} \tag{12}$$

which are used to reformulate the linear programming problem:

$$\begin{aligned} &\text{minimise} && y_X^{1,1} \\ &\text{subject to} && 0 \le y_X^{m,n} \le 1, \\ &&& e^{-(\mu_i+\mu_j)} \sum_{m,n=0}^{S_{\text{cut}}} \frac{\mu_i^m\mu_j^n}{m!n!} y_X^{m,n} \ge \max\left\{\underline{Q}_X^{\mu_i,\mu_j} - \gamma_{ij}, 0\right\}, \\ &&& e^{-(\mu_i+\mu_j)} \sum_{m,n=0}^{S_{\text{cut}}} \frac{\mu_i^m\mu_j^n}{m!n!} y_X^{m,n} \le \min\left\{\overline{Q}_X^{\mu_i,\mu_j}, 1\right\}, \end{aligned} \tag{13}$$

and

$$\begin{aligned} &\text{maximise} && b_X^{1,1} \\ &\text{subject to} && 0 \le b_X^{m,n} \le 1, \\ &&& e^{-(\mu_i+\mu_j)} \sum_{m,n=0}^{S_{\text{cut}}} \frac{\mu_i^m\mu_j^n}{m!n!} b_X^{m,n} \ge \max\left\{\underline{B}_X^{\mu_i,\mu_j} - \gamma_{ij}, 0\right\}, \\ &&& e^{-(\mu_i+\mu_j)} \sum_{m,n=0}^{S_{\text{cut}}} \frac{\mu_i^m\mu_j^n}{m!n!} b_X^{m,n} \le \min\left\{\overline{B}_X^{\mu_i,\mu_j}, 1\right\}. \end{aligned} \tag{14}$$

These problems can be solved to obtain $\underline{y}_X^{1,1}$ and $\overline{b}_X^{1,1}$, from which it follows $\overline{e}_X^{1,1} = \overline{b}_X^{1,1}/\underline{y}_X^{1,1}$ and $\underline{y}_Z^{1,1} = \underline{y}_X^{1,1} - \theta$, as discussed previously. Finally, to compute the key rate using Eqn. 1, we follow the approach in Ref. [5], defining the finite-size correction factor as $\Delta = 300.5/N_{\text{tot}}$ and redefining $q_Z^{1,1}$ as:

$$q_Z^{1,1} = \frac{1}{N_{\text{tot}}} \max\left\{|s^2e^{-2s}\underline{y}_Z^{1,1}\underline{N}_Z - g(s^2e^{-2s}\underline{y}_Z^{1,1}\underline{N}_Z, \epsilon_0)|, 0\right\}, \tag{15}$$

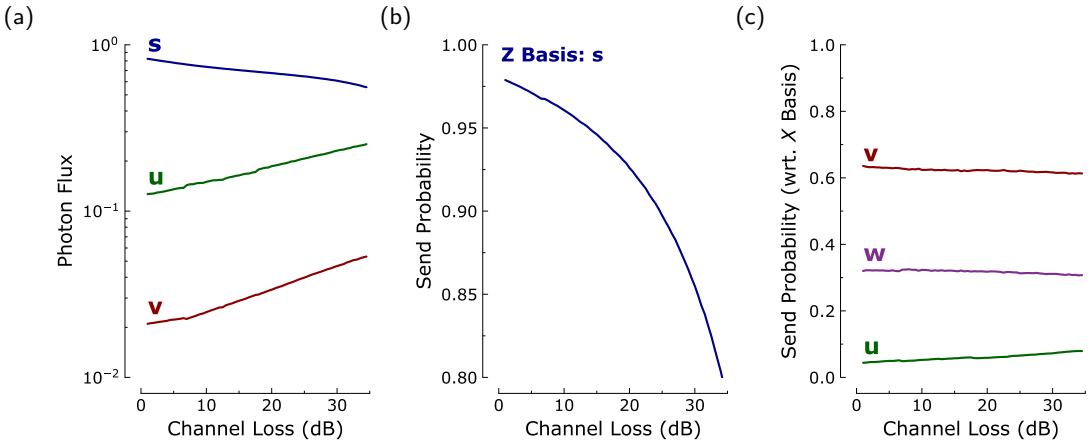
where N_{tot} is the total number of states transmitted in the sample.

SUPPLEMENTARY NOTE 3: PARAMETER OPTIMISATION

For optimum QKD system performance, it is important to carefully select all operating parameters in order to maximise the secure key rate. While general best-practice trends are known, for example, biasing basis selection to prepare the majority of states in the Z (key-generating) basis, the exact optimal parameters vary for each experimental implementation and also depend on the channel loss. Therefore, a full optimisation procedure is necessary to obtain the best possible results.

In the four-state decoy-state MDI-QKD protocol, we are required to optimise the intensities of s, u, v and w, in addition to the probabilities of the users choosing to prepare and transmit each state. The probabilities of state preparation are the same for each user and the requirement for unity sum of probabilities removes one degree of freedom. Additionally, to simplify the problem, we also fix the vacuum intensity to $w = 2 \times 10^{-4}$. This still leaves six parameters to optimise in our system, which is non-trivial and beyond the scope of a simple exhaustive parameter space search approach.

We therefore perform a full numerical optimisation by noting that the problem is convex and using a local optimisation algorithm, bounded to experimentally practical intensities and probabilities in the range $(0, 1)$. The algorithm is provided with a fitness function to maximise, comprising the secure key rate calculation in the finite-size regime with composable security where the gain and QBER are determined by simulating the protocol using the six optimisation variables in addition to experimentally measured component values. Supplementary Fig. 2 shows the optimised parameters, which were then used in our experiments (see main text), resulting in strong agreement between theoretically modelled and measured key rates.



Supplementary Figure 2. Numerically optimised parameters for our MDI-QKD system (including finite size effects, with composable security) with respect to total channel losses: (a) state intensities (w was fixed as $2{\times}10^{-4}$); (b) probability of encoding bit in Z basis (signal state s); (c) probability of encoding a u, v or w decoy state in the X basis (note that probabilities are plotted relative to the probably of encoding in the X basis).

SUPPLEMENTARY TABLES

Supplementary Tables I–III report detailed experimental results for our proof-of-principle MDI-QKD system at various channel loss values. Supplementary Table I presents the computed secure key rates using the three security analyses considered in this work, based on processing the raw experimental measurements obtained in the Z-basis (Table II) and X-basis (Table III). Supplementary Fig. 3 plots a selection of this data to show the measured gain and QBER for the cases where both parties send a bit either in the Z basis (s state) or the v state in the X basis (discussed in main text).

Channel Loss	**Secure Key Rate, R (bps)**		
	Asymptotic	**Finite Size**	**Finite Size with Composable Security**
30 dB (188 km)	2228	1971	1118
32 dB (200 km)	1607	1227	564
34 dB (213 km)	975	681	130
40 dB (250 km)	209	58	–
42 dB (263 km)	114	7	–
50 dB (313 km)	24	–	–
54 dB (338 km)	8	–	–

Supplementary Table I. Experimental secure key rates R, with respect to total channel attenuation (dB). In parentheses, we also report the equivalent distance in km, calculated by assuming ultra-low loss 0.16 dB km^{-1} fibre.

Z-Basis

Channel Loss	**Gain, $Q_Z^{s,s}$**	**QBER, $E_Z^{s,s}$**	**Flux, s**	**Prob., P_Z^s**
30 dB (188 km)	1.18×10^{-05}	1.07%	0.55	85.0%
32 dB (200 km)	8.75×10^{-06}	0.92%	0.60	83.0%
34 dB (213 km)	6.48×10^{-06}	0.84%	0.63	81.0%
40 dB (250 km)	1.85×10^{-06}	0.70%	0.63	81.0%
42 dB (263 km)	1.08×10^{-06}	0.63%	0.63	81.0%
50 dB (313 km)	1.70×10^{-07}	0.55%	0.63	81.0%
54 dB (338 km)	7.07×10^{-08}	0.55%	0.63	81.0%

Supplementary Table II. Experimental gains and errors in the Z-basis. These values were computed from the number of Bell state measurements, where the total prepared state sample size was $N_{\text{tot}} = 8.64 \times 10^{13}$ and the number of state preparations by the users is given by $N_Z^{s,s} = P_Z P_Z N_{\text{tot}}$. The QBER is observed to decrease slightly with increasing channel attenuation, which is attributed to reduced measurement jitter in SNSPDs at lower received count rates.

X-Basis

Channel Loss		Gain, $Q_X^{\mu_i,\mu_j}$				QBER, $E_X^{\mu_i,\mu_j}$			Flux, μ	Prob., P_X^μ
		u	v	w		u	v	w		
30 dB (188 km)	u	6.41×10^{-06}	2.44×10^{-06}	1.70×10^{-06}	u	26.9%	36.5%	48.5%	0.24	1.0%
	v	2.51×10^{-06}	2.94×10^{-07}	7.77×10^{-08}	v	36.5%	26.6%	48.2%	0.047	9.3%
	w	1.79×10^{-06}	7.59×10^{-08}	7.32×10^{-12}	w	48.5%	47.9%	32.5%	0.0002	4.7%
32 dB (200 km)	u	4.32×10^{-06}	1.67×10^{-06}	1.14×10^{-06}	u	26.6%	35.4%	48.5%	0.25	1.2%
	v	1.78×10^{-06}	2.38×10^{-07}	6.42×10^{-08}	v	35.4%	26.6%	48.2%	0.053	10.3%
	w	1.19×10^{-06}	5.80×10^{-08}	4.82×10^{-12}	w	48.5%	48.0%	43.0%	0.0002	5.5%
34 dB (213 km)	u	2.53×10^{-06}	9.95×10^{-07}	6.66×10^{-07}	u	26.5%	35.0%	48.5%	0.24	1.3%
	v	1.05×10^{-06}	1.63×10^{-07}	4.56×10^{-08}	v	34.5%	26.6%	48.6%	0.056	11.4%
	w	7.02×10^{-07}	3.87×10^{-08}	3.75×10^{-12}	w	48.4%	48.5%	44.6%	0.0002	6.3%
40 dB (250 km)	u	7.29×10^{-07}	2.73×10^{-07}	1.78×10^{-07}	u	26.8%	35.0%	48.6%	0.24	1.3%
	v	2.97×10^{-07}	4.30×10^{-08}	1.10×10^{-08}	v	35.2%	26.8%	48.1%	0.056	11.4%
	w	1.95×10^{-07}	1.06×10^{-08}	1.07×10^{-12}	w	48.5%	48.5%	22.6%	0.0002	6.3%
42 dB (263 km)	u	4.47×10^{-07}	1.68×10^{-07}	1.10×10^{-07}	u	26.9%	35.0%	48.6%	0.24	1.3%
	v	1.85×10^{-07}	2.62×10^{-08}	6.73×10^{-09}	v	35.4%	27.1%	48.1%	0.056	11.4%
	w	1.18×10^{-07}	6.46×10^{-09}	6.89×10^{-13}	w	48.7%	47.7%	42.9%	0.0002	6.3%
50 dB (313 km)	u	7.13×10^{-08}	2.61×10^{-08}	1.69×10^{-08}	u	27.1%	35.2%	49.2%	0.24	1.3%
	v	2.93×10^{-08}	4.15×10^{-09}	9.27×10^{-10}	v	34.8%	26.7%	48.5%	0.056	11.4%
	w	1.91×10^{-08}	1.04×10^{-09}	3.91×10^{-14}	w	48.8%	49.3%	49.5%	0.0002	6.3%
54 dB (338 km)	u	2.91×10^{-08}	1.06×10^{-08}	6.82×10^{-09}	u	26.9%	33.8%	48.2%	0.24	1.3%
	v	1.18×10^{-08}	1.69×10^{-09}	4.04×10^{-10}	v	35.4%	26.7%	49.1%	0.056	11.4%
	w	7.89×10^{-09}	4.33×10^{-10}	3.91×10^{-14}	w	49.0%	46.0%	49.5%	0.0002	6.3%

Supplementary Table III. Experimental gains and errors in the X-basis. These values were computed from the number of Bell state measurements for each state combination, where the total prepared state sample size was $N_{\rm tot} = 8.64 \times 10^{13}$ and the number of state preparations by the users is given by $N_X^{\mu_i,\mu_j} = P_X^{\mu_i} P_X^{\mu_j} N_{\rm tot}$.

[1] Yuan, Z. L. *et al.* Robust random number generation using steady-state emission of gain-switched laser diodes. *Appl. Phys. Lett.* **104**, 261112 (2014).

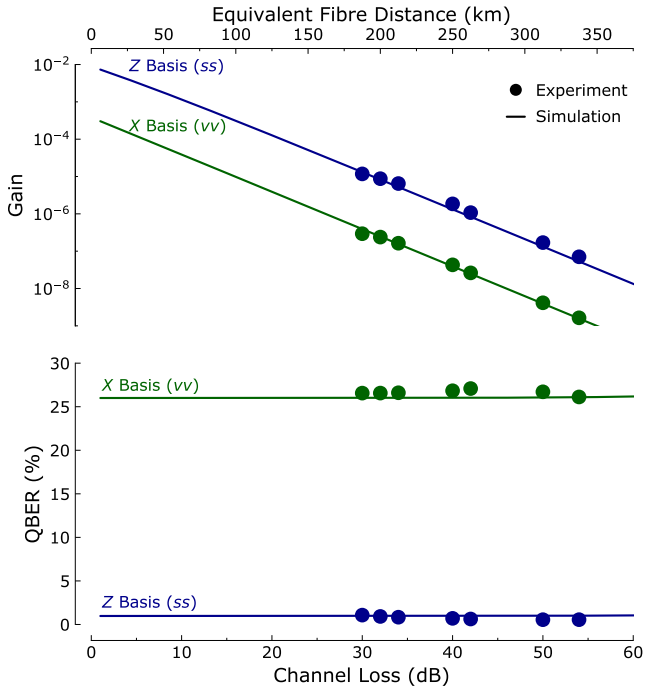
[2] Zhou, Y.-H., Yu, Z.-W. & Wang, X.-B. Making the decoy-state measurement-device-independent quantum key distribution practically useful. *Phys. Rev. A* **93**, 042324 (2016).

[3] Ma, X., Fung, C. H. F. & Razavi, M. Statistical fluctuation analysis for measurement-device-independent quantum key distribution. *Phys. Rev. A* **86**, 052305 (2012).

[4] Curty, M. *et al.* Finite-key analysis for measurement-device-independent quantum key distribution. *Nat. Commun.* **5**, 3732 (2014).

[5] Comandar, L. C. *et al.* Quantum key distribution without detector vulnerabilities using optically seeded lasers. *Nat. Photonics* **10**, 312–315 (2016).

[6] Xu, F., Curty, M., Qi, B. & Lo, H.-K. Practical aspects of measurement-device-independent quantum key distribution. *New J. Phys.* **15**, 113007 (2013).



Supplementary Figure 3. Gain and QBER for the X-basis (decoy state v) and Z-basis (signal state s), as a function of total channel loss (equivalent fibre distance assuming ultra-low loss 0.16 dB km^{-1} fibre is also shown). Experimental data (circles) are in good agreement with numerical simulations (lines) based on our experimental parameters.