nature COMMUNICATIONS

ARTICLE

Received 4 Jul 2013 | Accepted 27 Mar 2014 | Published 29 Apr 2014

DOI: 10.1038/ncomms4732

Finite-key analysis for measurement-device-independent quantum key distribution

Marcos Curty[1], Feihu Xu[2], Wei Cui[2], Charles Ci Wen Lim[3], Kiyoshi Tamaki[4] & Hoi-Kwong Lo[2]

Quantum key distribution promises unconditionally secure communications. However, as practical devices tend to deviate from their specifications, the security of some practical systems is no longer valid. In particular, an adversary can exploit imperfect detectors to learn a large part of the secret key, even though the security proof claims otherwise. Recently, a practical approach—measurement-device-independent quantum key distribution—has been proposed to solve this problem. However, so far its security has only been fully proven under the assumption that the legitimate users of the system have unlimited resources. Here we fill this gap and provide a rigorous security proof against general attacks in the finite-key regime. This is obtained by applying large deviation theory, specifically the Chernoff bound, to perform parameter estimation. For the first time we demonstrate the feasibility of long-distance implementations of measurement-device-independent quantum key distribution within a reasonable time frame of signal transmission.

[1] El Telecomunicación, Department of Signal Theory and Communications, University of Vigo, Vigo E-36310, Spain. [2] Center for Quantum Information and Quantum Control, Department of Physics and Department of Electrical & Computer Engineering, University of Toronto, Toronto, Ontario, Canada M5S 3G4. [3] Group of Applied Physics, University of Geneva, Geneva CH-1211, Switzerland. [4] NTT Basic Research Laboratories, NTT Corporation, 3-1, Morinosato Wakamiya Atsugi-Shi, Kanagawa 243-0198, Japan. Correspondence and requests for materials should be addressed to M.C. (email: mcurty@com.uvigo.es).

It is unequivocal that quantum key distribution (QKD)[1,2] needs to bridge the gap between theory and practice. In theory, QKD offers perfect security. In practice, however, it does not, as most practical devices behave differently from the theoretical models assumed in the security proofs. As a result, we face implementation loopholes, or so-called side channels, which may be used by adversaries without being detected, as seen in recent attacks against certain commercial QKD systems[3–11].

There are two potential ways to guarantee security in the realization of QKD. The first is to develop mathematical models that perfectly match the behaviour of physical apparatuses, and then incorporate this information into a new security proof. While this is plausible in theory, unfortunately it is very hard to realize in practice, if not impossible. The second alternative is to design new protocols and develop security proof techniques that are compatible with a wide class of device imperfections. This allows us to omit an accurate characterization of real apparatuses. The most well-known example of such a solution is (full) device-independent QKD (diQKD)[12–16]. Here the legitimate users of the system (typically called Alice and Bob) treat their devices as two quasi 'black boxes'—that is, they need to know which elements their boxes contain, but not how they fully function[17]. The security of diQKD relies on the violation of a Bell inequality[18,19], which certifies the presence of quantum correlations. Despite its beauty, however, this approach is highly impractical because it requires a loophole-free Bell test that at the moment is still unavailable[20]. Also, its secret key rate at practical distances is very limited[21,22].

Very recently, a novel approach has been introduced, which is fully practical and feasible to implement. This scheme is known as measurement-device-independent QKD (mdiQKD)[23] and offers a clear avenue to bridge the gap between theory and practice. Its feasibility has been promptly demonstrated both in laboratories and via field tests[24–27]. It successfully removes all (existing and yet to be discovered) detector side channels[3,5,6,9–11], which, arguably, is the most critical part of most QKD implementations. Importantly, in contrast to diQKD, this solution does not require that Alice and Bob perform a loophole-free Bell test; it is enough if they prove the presence of entanglement in a quantum state that is effectively distributed between them, just like in standard QKD schemes[28]. In addition, now Alice and Bob may treat the measurement apparatus as a true 'black box', which may be fully controlled by the adversary. A slight drawback is that Alice and Bob need to characterize the quantum states (for example, the polarization degrees of freedom of phase-randomized weak coherent pulses (WCPs)) that they send through the channel. However, as this process can be verified in a protected environment outside the influence of the adversary, it is less likely to be a problem. For completeness, the readers can refer to ref. 29 where a characterization of the prepared states is no longer required.

Nevertheless, so far the security of mdiQKD has only been proven in the asymptotic regime[23], which assumes that Alice and Bob have access to an unlimited amount of resources, or in the finite regime but only against particular types of attacks[30,31]. In summary, until now, a rigorous security proof of mdiQKD that takes full account of the finite size effects[32–34] has appeared to be missing and, for this reason, the feasibility of long-distance implementations of mdiQKD within a reasonable time frame of signal transmission has remained undemonstrated.

The main contributions of this work are twofold. First, in contrast to existing heuristic results on mdiQKD, we provide, for the first time, a security proof in the finite-key regime that is valid against general attacks and satisfies the composability definition[35,36] of QKD. Second, we apply large deviation theory, specifically a multiplicative form of the Chernoff bound[37], to perform the parameter estimation step. The latter is crucial to demonstrate that a long-distance implementation of mdiQKD (for example, 150 km of optical fibre with 0.2 dB km^{-1}) is feasible within a reasonable time frame. To obtain high secret key rates in this scenario, it is common to use decoy state techniques[38–40], both for standard QKD protocols and mdiQKD. Here a key challenge is to estimate the transmittance and the quantum bit error rate (QBER) of the single-photon component of the signal at the presence of high losses (for example, 30 dB). We show that such an estimation problem can be solved using the Chernoff bound, as it provides good bounds for the above parameters even in the high-loss regime. We highlight that our results can be applied to other QKD protocols (for example, the standard decoy state BB84 protocol[38–40]) as well as to general experiments in quantum information.

Results

Security definition. Before stating the protocol, let us quickly review the security framework[35,36] that we are considering here. A general QKD protocol (executed by Alice and Bob) generates either a pair of bit strings S_{A} and S_{B}, or a symbol $\perp$ to indicate the abort of the protocol. In general, the string of Alice, S_{A}, can be quantum mechanically correlated with a quantum state that is held by the adversary. Mathematically, this situation is described by the classical quantum state

$$\rho_{\mathrm{AE}}=\sum_{s}|s\rangle\langle s|\otimes\rho_{\mathrm{E}}^{s},$$

where $\{|s\rangle\}_{s}$ denotes an orthonormal basis for Alice's system, and the subscript E indicates the system of the adversary.

Ideally, we say that a QKD protocol is secure if it satisfies two conditions, namely the correctness and the secrecy. The correctness condition is met if $S_{\mathrm{A}}=S_{\mathrm{B}}$, that is, Alice's and Bob's bit strings are identical. The secrecy condition is met if $\rho_{\mathrm{AE}}=U_{\mathrm{A}}\otimes\rho_{\mathrm{E}}$, where $U_{\mathrm{A}}=\sum_{s}\frac{1}{|S|}|s\rangle\langle s|$ is the uniform mixture of all possible values of the bit string S_{A}. That is, the system of the adversary is completely decoupled from that of Alice.

Owing to the presence of errors, however, these two conditions can never be perfectly met. For example, in the finite-key regime it is impossible to guarantee $S_{\mathrm{A}}=S_{\mathrm{B}}$ with certainty. In practice, this implies that we need to allow for some minuscule errors. That is, we say that a QKD scheme is ϵ_{cor}-correct if $\Pr[S_{\mathrm{A}}\neq S_{\mathrm{B}}]\leq\epsilon_{\mathrm{cor}}$, that is, the probability that Alice's and Bob's bit strings are not identical is not greater than ϵ_{cor}. Similarly, we say that a protocol is, ϵ_{sec}-secret if

$$\frac{1}{2}\|\rho_{\mathrm{AB}}-U_{\mathrm{A}}\otimes\rho_{\mathrm{E}}\|_{1}\leq\epsilon_{\mathrm{sec}},$$

where $\|\cdot\|_{1}$ denotes the trace norm. That is, the state ρ_{AB} is ϵ_{sec}-close to the ideal situation described by $U_{\mathrm{A}}\otimes\rho_{\mathrm{E}}$. Thereby a QKD protocol is said to be ϵ-secure if it is both ϵ_{cor}-correct and ϵ_{sec}-secret, with $\epsilon_{\mathrm{cor}}+\epsilon_{\mathrm{sec}}\leq\epsilon$.

With this security definition we are able to guarantee that the security of the protocol holds even when combined with other protocols, that is, the protocol is secure in the so-called universally composable framework[35,36].

Protocol definition. The set-up is illustrated in Fig. 1. Alice and Bob use a laser source to generate quantum signals that are diagonal in the Fock basis. Instances of such sources include attenuated laser diodes emitting phase-randomized WCPs, triggered spontaneous parametric downconversion sources and practical single-photon sources. Each pulse is prepared in a different BB84 state[41], which is selected, for example, uniformly at random from two mutually unbiased bases, denoted as Z and X. The signals are then sent to an untrusted relay Charles,

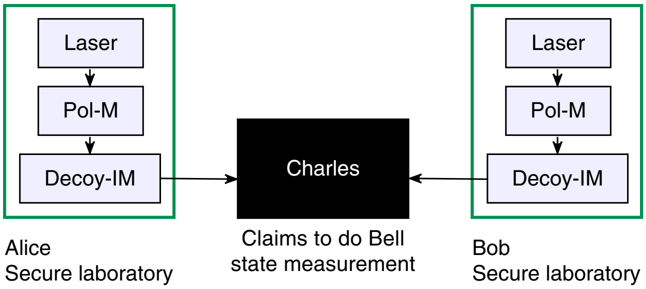

Figure 1 | A schematic diagram of mdiQKD. Alice and Bob prepare quantum signals in different BB84 polarization states[41] with a polarization modulator (Pol-M). Also, they use an intensity modulator (Decoy-IM) to generate decoy states. The signals are sent to an untrusted relay Charles, who is supposed to perform a Bell state measurement that projects the incoming signals into a Bell state. See the main text for details.

Box 1 | Protocol definition.

State preparation: Alice and Bob repeat the first four steps of the protocol for $i=1,\ldots,N$ until the conditions in the Sifting step are met. For each i, Alice chooses an intensity $a\in\{a_{\rm s}, a_{{\rm d}_1}, \ldots, a_{{\rm d}_n}\}$, a basis $\alpha\in\{{\rm Z},{\rm X}\}$, and a random bit $r\in\{0,1\}$ with probability $p_{a,\alpha}/2$. Here $a_{\rm s}\left(a_{{\rm d}_j}\right)$ is the intensity of the signal (decoy) states. Next, she generates a quantum signal (for example, a phase-randomized WCP) of intensity a prepared in the basis state of α given by r. Likewise, Bob does the same.
Distribution: Alice and Bob send their states to Charles via the quantum channel.
Measurement: If Charles is honest, he measures the signals received with a Bell state measurement. In any case, he informs Alice and Bob (via a public channel) of whether or not his measurement was successful. If successful, he reveals the Bell state obtained.
Sifting: If Charles reports a successful result, Alice and Bob broadcast (via an authenticated channel) their intensity and basis settings. For each Bell state k, we define two groups of sets: $\mathcal{Z}_k^{a,b}$ and $\mathcal{X}_k^{a,b}$. The first (second) one identifies signals where Charles declared the Bell state k and Alice and Bob selected the intensities a and b and the basis Z (X). The protocol repeats these steps until $\left|\mathcal{Z}_k^{a,b}\right|\geq N_k^{a,b}$ and $\left|\mathcal{X}_k^{a,b}\right|\geq M_k^{a,b}\ \forall a,b,k$. Next, say Bob flips part of his bits to correctly correlate them with those of Alice (see Table 1). Afterwards, they execute the last steps of the protocol for each k.
Parameter estimation: Alice and Bob use n_k random bits from $\mathcal{Z}_k^{a_{\rm s},b_{\rm s}}$ to form the code bit strings Z_k and Z'_k, respectively. The remaining R_k bits from $\mathcal{Z}_k^{a_{\rm s},b_{\rm s}}$ are used to compute the error rate $E_k^{a_{\rm s},b_{\rm s}}=\frac{1}{R_k}\sum_l r_l\oplus r'_l$, where r'_l are Bob's bits. If $E_k^{a_{\rm s},b_{\rm s}}>E_{\rm tol}$, Alice and Bob assign an empty string to S_k and abort steps 6 and 7 for this k. The protocol only aborts if $E_k^{a_{\rm s},b_{\rm s}}>E_{\rm tol}\,\forall k$. If $E_k^{a_{\rm s},b_{\rm s}}\leq E_{\rm tol}$, Alice and Bob use $\mathcal{Z}_k^{a,b}$ and $\mathcal{X}_k^{a,b}$ to estimate $n_{k,0}$, $n_{k,1}$ and $e_{k,1}$. The parameter $n_{k,0}$, ($n_{k,1}$) is a lower bound for the number of bits in Z_k where Alice (Alice and Bob) sent a vacuum (single-photon) state. $e_{k,1}$ is an upper bound for the single-photon phase error rate. If $e_{k,1}>e_{\rm tol}$, an empty string is assigned to S_k and steps 6 and 7 are aborted for this k, and the protocol only aborts if $e_{k,1}>e_{tol}\,\forall k$.
Error correction: For those k that passed the parameter estimation step, Bob obtains an estimate $\hat{Z}_k$ of Z_k using an information reconciliation scheme. For this, Alice sends him ${\rm leak}_{{\rm EC},k}$ bits of error correction data. Next, Alice computes a hash of Z_k of length $\lceil\log_2(4/\epsilon_{\rm cor})\rceil$ using a random universal$_2$ hash function, which she sends to Bob together with the hash[35]. If ${\rm hash}(\hat{Z}_k)\neq{\rm hash}(Z_k)$, Alice and Bob assign an empty string to S_k and abort step 7 for this k. The protocol only aborts if ${\rm hash}(\hat{Z}_k)\neq{\rm hash}(Z_k)\,\forall k$.
Privacy amplification: If k passed the error correction step, Alice and Bob apply a random universal$_2$ hash function to Z_k and $\hat{Z}_k$ to extract two shorter strings of length ℓ_k (see ref. 35). Alice obtains S_k and Bob $\hat{S}_k$. The concatenation of $S_k\left(\hat{S}_k\right)$ form the secret key $S_{\rm A}$ ($S_{\rm B}$).

Table 1 | Post-processing of data in the sifting step.

Alice & Bob	Bell state reported by Charles			
	$\lvert\psi^-\rangle$	$\lvert\psi^+\rangle$	$\lvert\phi^-\rangle$	$\lvert\phi^+\rangle$
Z basis	Bit flip	Bit flip	—	—
X basis	Bit flip	—	Bit flip	—

To guarantee that their bit strings are correctly correlated, say Bob applies a bit flip to part of his data, depending on the Bell state reported by Charles and the basis setting selected.

who is supposed to perform a Bell state measurement that projects them into a Bell state. Also, Alice and Bob apply decoy state techniques[38–40] to estimate the gain (that is, the probability that the relay outputs a successful result) and the QBER for various input photon numbers.

Next, Charles announces whether or not his measurements are successful, including the Bell states obtained. Alice and Bob keep the data that correspond to these instances and discard the rest. Also, they post-select the events where they employ the same basis. Finally, either Alice or Bob flips part of her/his bits to correctly correlate them with those of the other. See Box 1 for a detailed description of the different steps of the protocol.

Since Charles' measurement is basically used to post-select entanglement between Alice and Bob, the security of mdiQKD can be proven by using the idea of time reversal. Indeed, mdiQKD builds on the earlier proposals of time-reversed EPR protocols by Biham *et al.*[42] and Inamori[43], and combine them with the decoy state technique. The end result is the best of both worlds—high performance and high security. We note on passing that the idea of time reversal has also been previously used in other quantum information protocols including one-way quantum computation.

Security analysis. We now present one main result of our paper. It states that the protocol introduced above is both $\epsilon_{\rm cor}$-correct and $\epsilon_{\rm sec}$-secret, given that the length ℓ of the secret key $S_{\rm A}$ is selected appropriately for a given set of observed values. See Box 1 for the definition of the different parameters that we consider in this section.

The correctness of the protocol is guaranteed by its error correction step, where, for each possible Bell state k, Alice sends a hash of Z_k to Bob, who compares it with the hash of $\hat{Z}_k$. If both hash values are equal, the protocol gives $S_k{=}\hat{S}_k$ except with error probability $\epsilon_{\rm cor}/4$. If ${\rm hash}(\hat{Z}_k)\neq{\rm hash}(Z_k)$, its output is an empty string (that is, the protocol is trivially correct). Moreover, if the protocol aborts, the result is $\perp$, that is, it is also correct. This guarantees that $S_{\rm A}=S_{\rm B}$ except with error probability $\leq\epsilon_{\rm cor}$. Alternatively to this method, Alice and Bob may also guarantee the correctness of the protocol by exploiting properties of the error-correcting code employed[44].

If the length ℓ_k of each bit string S_k, which forms the secret key $S_{\rm A}$, satisfies

$$\begin{aligned}\ell_k\leq & n_{k,0}+n_{k,1}\left[1-h\left(e_{k,1}\right)\right]-{\rm leak}_{{\rm EC},k}\\ & -\log_2\frac{8}{\epsilon_{\rm cor}}-2\log_2\frac{2}{\varepsilon'_k\hat{\varepsilon}_k}-2\log_2\frac{1}{2\varepsilon_{k,{\rm PA}}},\end{aligned}\qquad(1)$$

the protocol is $\epsilon_{\rm sec}$-secret, with $\epsilon_{\rm sec}=\sum_k\epsilon_{k,{\rm sec}}$ and $\epsilon_{k,{\rm sec}}=2(\varepsilon'_k+2\varepsilon_{k,e}+\hat{\varepsilon}_k)+\varepsilon_{k,b}+\varepsilon_{k,0}+\varepsilon_{k,1}+\varepsilon_{k,{\rm PA}}$. In equation (1), $h(x)=-x\log_2(x)-(1-x)\log_2(1-x)$ is the binary Shannon entropy, and the parameters $\varepsilon_{k,0}$, $\varepsilon_{k,1}$, and $\varepsilon_{k,e}$ quantify, respectively, the probability that the estimation of the terms $n_{k,0}$, $n_{k,1}$ and $e_{k,1}$ is incorrect. A sketch of the proof of equation (1) can be found in the Methods section. Also explained there, is the meaning of all the epsilons contained in the term $\epsilon_{k,{\rm sec}}$, which we omit here for simplicity. In the asymptotic limit of very large data blocks, the terms reducing the length of S_A due to statistical fluctuations may be neglected, and thus ℓ satisfies $\ell \leq \sum_k \max\{n_{k,0} + n_{k,1}[1 - h(e_{k,1})] - \text{leak}_{\text{EC},k}, 0\}$, as previously obtained in ref. 23. That is, $n_{k,0}$ and $n_{k,1}$ provide a positive contribution to the secret key rate, while $n_{k,1}h(e_{k,1})$ and $\text{leak}_{\text{EC},k}$ reduce it. The term $n_{k,1}h(e_{k,1})$ corresponds to the information removed from Z_k in the privacy amplification step of the protocol, while $\text{leak}_{\text{EC},k}$ is the information revealed by Alice in the error correction step.

The second main contribution of this work is an estimation method to obtain the relevant parameters $n_{k,0}$, $n_{k,1}$ and $e_{k,1}$ needed to evaluate the key rate formula above, when Alice and Bob send Charles a finite number, N, of signals and use a finite number of decoy states. We solve this problem using techniques in large deviation theory. More specifically, we employ the Chernoff bound[37]. It is important to note that standard techniques such as Azuma's inequality[45] do not give very good bounds here. This is because this result does not consider the properties of the *a priori* distribution. Therefore, it is far from optimal for situations such as high loss or a highly bias coin flip, which are relevant in long-distance QKD. In contrast, the Chernoff bound takes advantage of the property of the distribution and provides good bounds even in a high-loss regime.

More precisely, we show that the estimation of $n_{k,0}$, $n_{k,1}$ and $e_{k,1}$ can be formulated as a linear program, which can be solved efficiently in polynomial time and gives the exact optimum even for large dimensions[46]. Importantly, this general method is valid for any finite number of decoy states used by Alice and Bob, and for any photon-number distribution of their signals. Also, for the typical scenario where Alice and Bob send phase-randomized WCPs together with two decoy states each, we solve analytically the linear program, and obtain analytical expressions for the parameters above, which can be used directly in an experiment. A sketch of the estimation technique is given in the Methods section. For a detailed analysis of both estimation techniques we refer to the Supplementary Notes 1 and 2.

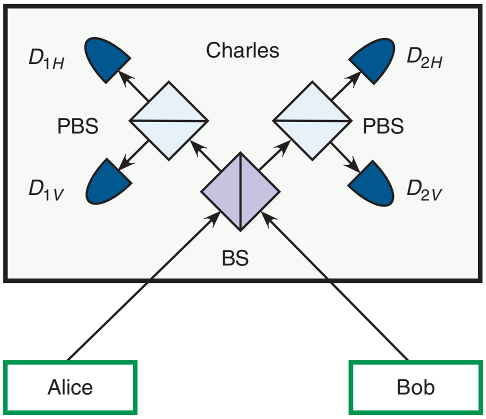

Figure 2 | A schematic diagram of Charles' measurement device. The signals from Alice and Bob interfere at a 50:50 beam splitter (BS), which has on each end a polarizing beam splitter (PBS) that projects the incoming photons into either horizontal (H) or vertical (V) polarization states. A click in the single-photon detectors D_{1H} and D_{2V}, or in D_{1V} and D_{2H}, indicates a projection into the Bell state $|\psi^-\rangle = 1/\sqrt{2}(|HV\rangle - |VH\rangle)$, while a click in D_{1H} and D_{1V}, or in D_{2H} and D_{2V}, implies a projection into the Bell state $|\psi^+\rangle = 1/\sqrt{2}(|HV\rangle + |VH\rangle)$.

Discussion

In this section, we analyse the behaviour of the secret key rate provided in equation (1). In our simulation, we consider that Alice and Bob encode their bits in the polarization degrees of freedom of phase-randomized WCPs. Also, we assume that Charles uses the linear optics quantum relay illustrated in Fig. 2, which is able to identify two of the four Bell states. With this set-up, a successful Bell state measurement corresponds to the observation of precisely two detectors (associated to orthogonal polarizations) being triggered. Note, however, that the results presented in this paper can be applied to other types of coding schemes like, for instance, phase or time-bin coding[1,2], and to any quantum operation that Charles may perform, as they solely depend on the measurement results that he announces.

We use experimental parameters from ref. 47. But, whereas ref. 47 considers a free-space channel, we assume a fibre-based channel with a loss of 0.2 dB km^{-1}. The detection efficiency of the relay (that is, the transmittance of its optical components together with the efficiency of its detectors) is 14.5% and the background count rate is 6.02×10^{-6}. Moreover, we use a rather generic channel model that includes an intrinsic error rate that simulates the misalignment and instability of the optical system. This is done by placing a unitary rotation in both input arms of the 50:50 beam splitter, and another unitary rotation in one of its output arms[48]. In addition, we fix the security bound to $\epsilon = 10^{-10}$.

The results are shown in Figs 3 and 4 for the situation where Alice and Bob use two decoy states each. In this scenario, we obtain the parameters $n_{k,0}$, $n_{k,1}$ and $e_{k,1}$ using the analytical estimation procedure introduced above (see Supplementary Note 1 for more details). The first figure illustrates the secret key rate (per pulse) ℓ/N as a function of the distance between Alice and Bob for different values of the total number of signals N

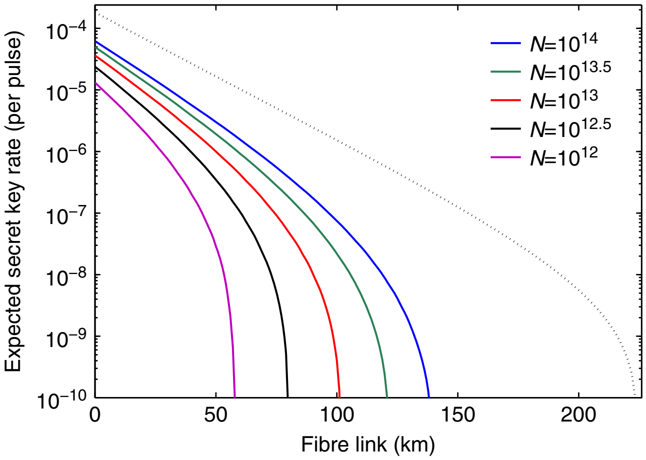

Figure 3 | Expected key rate as function of the distance. Secret key rate ℓ/N in logarithmic scale for the protocol introduced in the Results section with phase-randomized WCPs as a function of the distance. The solid lines correspond to different values for the total number of signals N sent by Alice and Bob. The overall misalignment in the channel is 1.5%, and the security bound $\epsilon = 10^{-10}$. For simulation purposes we consider the following experimental parameters[47]: the loss coefficient of the channel is 0.2 dB km^{-1}, the detection efficiency of the relay is 14.5% and the background count rate is 6.02×10^{-6}. Our results show clearly that even with a realistic finite size of data, say $N = 10^{12}$ to 10^{14}, it is possible to achieve secure mdiQKD at long distances. In comparison, the dotted line represents a lower bound on the secret key rate for the asymptotic case where Alice and Bob send Charles infinite signals and use an infinite number of decoy settings.

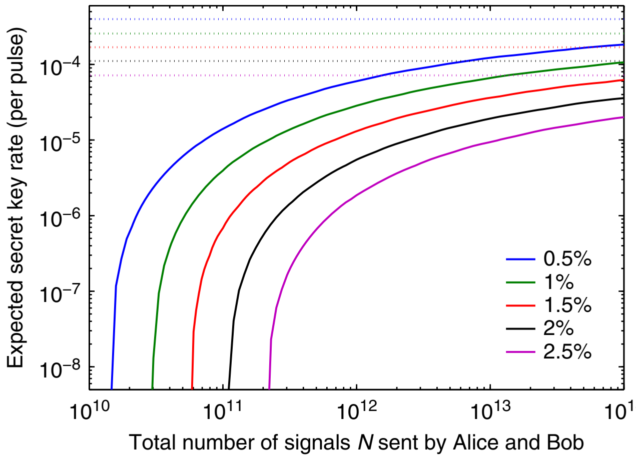

Figure 4 | Expected key rate as function of the block size. The plot shows the secret key rate ℓ/N in logarithmic scale as a function of the total number of signals N sent by Alice and Bob in the limit of zero distance. The security bound $\epsilon = 10^{-10}$. The solid lines correspond to different values for the intrinsic error rate due to the misalignment and instability of the optical system. The horizontal dotted lines show the asymptotic rates. The experimental parameters are the ones described in the caption of Fig. 3. Our results show that, even for a finite size of signals sent by Alice and Bob, mdiQKD is robust to intrinsic errors due to basis misalignment and instability of the optical system.

sent. We fix $\epsilon_{\rm cor} = 10^{-15}$; this corresponds to a realistic hash tag size in practice[35]. Also, we fix the intensity of the weakest decoy states to $a_{\rm d_2} = b_{\rm d_2} = 5\times10^{-4}$, since, in practice, it is difficult to generate a vacuum state due to imperfect extinction. This value for $a_{\rm d_2}$ and $b_{\rm d_2}$ can be easily achieved with a standard intensity modulator. Moreover, for simplicity, we assume an error correction leakage that is a fixed fraction of the sifted key length n_k, that is, ${\rm leak}_{{\rm EC},k}{=}n_k\zeta h(E_k^{a_{\rm s},b_{\rm s}})$, with $\zeta = 1.16$ and where $h(\cdot)$ is again the binary Shannon entropy[32]. In a realistic scenario, however, the value of ζ typically depends on the value of n_k, and when $n_k < 10^5$ the parameter ζ may be bigger than 1.16. For a given distance, we optimize numerically ℓ/N over all the free parameters of the protocol. This includes the intensities $a_{\rm s}$, $a_{\rm d_1}$, $b_{\rm s}$ and $b_{\rm d_1}$, the probability distributions $p_{a,\alpha}$ and $p_{b,\beta}$ in the state preparation step, the parameters $N_k^{a,b}$ and $M_k^{a,b}$ in the sifting step, the term n_k in the parameter estimation step and the different epsilons contained in $\epsilon_{\rm sec}$. Our simulation result shows clearly that mdiQKD is feasible with current technology and does not require high-efficiency detectors for its implementation. If Alice and Bob use laser diodes operating at 1 GHz repetition rate, and each of them sends $N = 10^{13}$ signals, we find, for instance, that they can distribute a 1-Mb secret key over a 75-km fibre link in <3 h. This scenario corresponds to the red line shown in Fig. 3. Notice that, at telecom wavelengths, standard InGaAs detectors have modest detection efficiency of about 15%. Since mdiQKD requires twofold coincidence rather than single detection events, as is the case in the standard decoy state protocol, the key rate of mdiQKD is lower than that of the standard decoy state scheme. However, with high-efficiency detectors such as silicon detectors[49] in 800 nm or high-efficiency superconducting nanowire single-photon detectors[50], the key rate of mdiQKD can be made comparable to that of the standard decoy state protocol.

The second figure illustrates ℓ/N as a function of N for different values of the misalignment in the limit of zero distance. For comparison, this figure also includes the asymptotic secret key rate when Alice and Bob send an infinite number of signals and use an infinite number of decoy states[23]. Our results show that significant secret key rates are already possible with 10^{11} signals, given that the error rate is not too large.

In conclusion, we have proved the security of mdiQKD in the finite-key regime against general attacks. This is the only known fully practical QKD protocol that offers an avenue to bridge the gap between theory and practice in QKD implementations. Importantly, our results clearly demonstrate that even with practical signals (for example, phase-randomized WCPs) and a finite size of data (say 10^{12} to 10^{14} signals) it is possible to perform secure mdiQKD over long distances (up to about 150 km).

To achieve high secret key rates in such high-loss regime, it is typical for both standard QKD schemes and mdiQKD to use decoy state techniques. A main challenge in this scenario is to obtain tight bounds for the gain and QBER of the single-photon components sent by Alice and Bob. We have shown that this estimation problem can be successfully solved using techniques in large deviation theory, more precisely, the Chernoff bound. This result takes advantage of the property of the distribution, and thus provides good bounds for the relevant parameters even in the presence of high losses, as is the case in QKD realizations.

Using the Chernoff bound, we have rewritten the problem of estimating the gain and QBER of the single-photon signals as a linear program, which can be solved efficiently in polynomial time. This general method is valid for any finite number of decoy states, and for any photon-number distribution of the signals. It can be used, for instance, with laser diodes emitting phase-randomized WCPs, triggered spontaneous parametric downconversion sources and practical single-photon sources. Also, for the common scenario where Alice and Bob send phase-randomized WCPs together with two decoy states each, we have obtained tight analytical bounds for the quantities above. These results apply to different types of coding schemes like, for example, polarization, phase or time-bin coding.

Methods

Secrecy. Here we briefly discuss on the secrecy of the protocol described in Box 1. To begin with, note that Alice and Bob obtain the error rate $E_k^{a_{\rm s},b_{\rm s}}$ using a random sample of $\mathcal{Z}_k^{a_{\rm s},b_{\rm s}}$ of size R_k. This means that when $E_k^{a_{\rm s},b_{\rm s}}$ satisfies the tolerated value $E_{\rm tol}$, the error rate between the strings Z_k and Z'_k, which we denote as $\xi_k^{a_{\rm s},b_{\rm s}}$, satisfies the following inequality written as conditional probability[51]

$$\Pr\left[\xi_k^{a_{\rm s},b_{\rm s}} \geq E_k^{a_{\rm s},b_{\rm s}} + \chi(n_k, R_k, \bar{\varepsilon}_k) \mid \Omega_{\rm pass}\right] \leq \bar{\varepsilon}_k^2, \qquad (2)$$

where $\chi(x,y,z){=}\sqrt{(y+x)(y+1)/(xy^2)\ln z^{-1}}$. Here the parameter $\Omega_{\rm pass}$ represents the event that all the tests performed during the realization of the protocol satisfy the tolerated values.

Let E'_k denote the adversary's information about Z_k up to the error correction step in Box 1. By using a privacy amplification scheme based on two-universal hashing[35] we can generate an ϵ_k-secret string S_k of length ℓ_k, where $\varepsilon_k > 0$, and

$$\epsilon_k \leq 8\varepsilon_k + 2^{-\frac{1}{2}\left(H_{\rm min}^{4\varepsilon_k}\left(Z_k|E'_k\right) - \ell_k\right) - 1}. \qquad (3)$$

The function $H_{\rm min}^{4\varepsilon_k}\left(Z_k \mid E'_k\right)$ denotes the smooth min-entropy[35,52]. It quantifies the average probability that the adversary guesses Z_k correctly using the optimal strategy with access to E'_k.

The term E'_k can be decomposed as $E'_k{=}C_kE_k$, where C_k is the information revealed by Alice and Bob during the error correction step, and E_k is the adversary's information before that step. Using a chain rule for smooth entropies[35], we obtain

$$H_{\rm min}^{4\varepsilon_k}\left(Z_k \mid E'_k\right) \geq H_{\rm min}^{4\varepsilon_k}(Z_k \mid E_k) - |C_k|, \qquad (4)$$

with $|C_k| \leq {\rm leak}_{{\rm EC},k} + \log_2(8/\epsilon_{\rm cor})$.

The bits of Z_k can be distributed among three different strings: Z_k^0, Z_k^1 and $Z_k^{\rm rest}$. The first contains bits where Alice sent a vacuum state, the second where both Alice and Bob sent a single-photon state and $Z_k^{\rm rest}$ includes the rest of bits. Using the result from ref. 53, we have that

$$\begin{aligned} H_{\rm min}^{4\varepsilon_k}(Z_k \mid E_k) &\geq H_{\rm min}^{\varepsilon'_k + 2\varepsilon''_k + (\hat{\varepsilon}_k + 2\hat{\varepsilon}'_k + \hat{\varepsilon}''_k)}\left(Z_k^0 Z_k^1 Z_k^{\rm rest} \mid E_k\right) \\ &\geq n_{k,0} + H_{\rm min}^{\varepsilon''_k}\left(Z_k^1 \mid Z_k^0 Z_k^{\rm rest} E_k\right) - 2\log_2\frac{2}{\varepsilon'_k \hat{\varepsilon}_k}, \end{aligned} \qquad (5)$$

where $4\varepsilon_k{=}\varepsilon'_k + 2\varepsilon''_k + \left(\hat{\varepsilon}_k + 2\hat{\varepsilon}'_k + \hat{\varepsilon}''_k\right)$. Here we have used the fact that $H_{\rm min}^{\hat{\varepsilon}'_k}\left(Z_k^{\rm rest} \mid Z_k^0 E_k\right) \geq 0$, and $H_{\rm min}^{\hat{\varepsilon}''_k}\left(Z_k^0 \mid E_k\right) \geq H_{\rm min}^0\left(Z_k^0 \mid E_k\right){=}H_{\rm min}\left(Z_k^0\right){=}n_{k,0}$.

The latter arises because vacuum states contain no information about their bit values, which are uniformly distributed.

The next step is to obtain a lower bound for the term $H_{\min}^{\varepsilon_k''}(Z_k^1 \mid Z_k^0 Z_k^{\text{rest}} E_k)$. Taking that Alice and Bob do the state preparation scheme perfectly in the Z and X bases (that is, they prepare perfect BB84 states), we can re-write this quantity in terms of the smooth max-entropy between them, which is directly bounded by the strength of their correlations[32]. More precisely, the entropic uncertainty relation gives us

$$H_{\min}^{\varepsilon_k''}(Z_k^1 \mid Z_k^0 Z_k^{\text{rest}} E_k) \geq n_{k,1} - H_{\max}^{\varepsilon_k''}\left(X_k^1 \mid {X'}_k^1\right) \geq n_{k,1} - n_{k,1} h\left(e_{k,1}\right). \tag{6}$$

Combining equations (3)–(6), we find that a secret key of length ℓ_k given by equation (1) gives an error of $\epsilon_k \leq 2\left(\varepsilon_k' + 2\varepsilon_k'' + \hat{\varepsilon}_k + 2\hat{\varepsilon}_k' + \hat{\varepsilon}_k''\right) + \varepsilon_{k,\text{PA}}$. Finally, after composing the errors related with the estimation of $n_{k,0}$, $n_{k,1}$ and $e_{k,1}$, selecting $\hat{\varepsilon}_k'$ and $\hat{\varepsilon}_k''$ equal to zero, and also removing the conditioning on Ω_{pass}, we obtain a security parameter $\epsilon_{k,\text{sec}}$ given by

$$\epsilon_{k,\text{sec}} = 2\left(\varepsilon_k' + 2\varepsilon_{k,e} + \hat{\varepsilon}_k\right) + \varepsilon_{k,\text{b}} + \varepsilon_{k,0} + \varepsilon_{k,1} + \varepsilon_{k,\text{PA}}, \tag{7}$$

where $\varepsilon_{k,\text{b}} = \bar{\varepsilon}_k \sqrt{\Pr\left[\Omega_{\text{pass}}\right]}$, and $\varepsilon_{k,0}$, $\varepsilon_{k,1}$ and $\varepsilon_{k,e}$, denote, respectively, the error probability in the estimation of $n_{k,0}$, $n_{k,1}$ and $e_{k,1}$.

Parameter estimation. To simplify the discussion, let us consider the estimation of the parameter $n_{k,0}$. The method to obtain $n_{k,1}$ and $e_{k,1}$ follows similar arguments. The procedure can be divided into two steps. First, we calculate a lower bound for the number of indexes in $\mathcal{Z}_k^{a_s,b_s}$ where Alice sent a vacuum state. This quantity is denoted as $m_{k,0}$. Second, we compute $n_{k,0}$ from $m_{k,0}$ using the Serfling inequality for random sampling without replacement[51].

In the first step we use a multiplicative form of the Chernoff bound[37] for independent random variables, which does not require the prior knowledge on the population mean. More precisely, we use the following claim.

Claim: Let $X_1, X_2, \ldots, X_n$, be a set of independent Bernoulli random variables that satisfy $\Pr(X_i = 1) = p_i$, and let $X = \sum_{i=1}^n X_i$ and $\mu = E[X] = \sum_{i=1}^n p_i$, where $E[\cdot]$ denotes the mean value. Let x be the observed outcome of X for a given trial (that is, $x \in \mathbb{N}^+$) and $\mu_{\text{L}} = x - \sqrt{n/2 \ln(1/\epsilon)}$ for certain $\epsilon > 0$. When $(2\varepsilon^{-1})^{1/\mu_{\text{L}}} \leq \exp\left[3/(4\sqrt{2})\right]^2$ and $(\hat{\varepsilon}^{-1})^{1/\mu_{\text{L}}} < \exp(1/3)$ for a certain $\varepsilon, \hat{\varepsilon} > 0$, we have that x satisfies

$$x = \mu + \delta, \tag{8}$$

except with the error probability $\gamma = \epsilon + \varepsilon + \hat{\varepsilon}$, where the parameter $\delta \in \left[-\Delta, \hat{\Delta}\right]$, with $\Delta = g(x, \varepsilon^4/16)$, $\hat{\Delta} = g\left(x, \hat{\varepsilon}^{3/2}\right)$ and $g(x, y) = \sqrt{2x \ln(y^{-1})}$. Here $\varepsilon(\hat{\varepsilon})$ denotes the probability that $x < \mu - \Delta \left(x > \mu + \hat{\Delta}\right)$.

Importantly, the bounds ($-\Delta$ and $\hat{\Delta}$) on the fluctuation parameter δ that appears in equation (8) do not depend on the mean value μ. A proof of this claim can be found in the Supplementary Note 3. There we introduce as well a generalized version of the claim for the cases where $(2\varepsilon^{-1})^{1/\mu_{\text{L}}} > \exp\left[3/4\sqrt{2}\right]^2$ and/or $(\hat{\varepsilon}^{-1})^{1/\mu_{\text{L}}} \geq \exp(1/3)$.

To apply this statement and be able to obtain the parameter $m_{k,0}$, we rephrase the protocol described in Box 1. For each signal, we consider that Alice (Bob) first chooses a photon-number $n(m)$ and sends the signal to Charles, who declares whether his measurement is successful or not. After Alice decides the intensity setting a, Bob does the same. This virtual protocol is equivalent to the original one because the essence of decoy state QKD is precisely that Alice and Bob could have postponed the choice of which states are signals or decoys after Charles' declaration of the successful events. This is possible because Alice's and Bob's observables commute with those of Charles. Note that for each specific combination of values n and m, the observables that Alice and Bob use to determine whether a state is a signal or a decoy act on entirely different physical systems from those of Charles. This implies that Alice and Bob are free to postpone their measurement and thus their choice of signals and decoys. Also, this result shows that for each combination n and m, the signal and decoy states provide a random sample of the population of all signals containing n and m photons, respectively. Therefore, one can apply random sampling theory in classical statistics to the quantum problem.

Let $\mathcal{S}_{k,nm}$ denote the set that identifies those signals sent by Alice and Bob with n and m photons, respectively, when they select the Z basis and Charles announces the Bell state k. And, let $\left|\mathcal{S}_{k,nm}\right| = \mathcal{S}_{k,nm}$, and $p_{a,b|nm,\text{Z}}$ be the conditional probability that Alice and Bob have selected the intensity settings a and b, given that their signals contain, respectively, n and m photons prepared in the Z basis. Then, if we apply the above equivalence, independently of each other and for each signal Alice and Bob assign to each element in $\mathcal{S}_{k,nm}$ the intensity setting a, b, with probability $p_{a,b|nm,\text{Z}}$.

Let $X_{i|k,nm}^{a,b}$ be 1 if the ith element of $\mathcal{S}_{k,nm}$ is assigned to the intensity setting combination a, b, and otherwise 0. And, let

$$X_k^{a,b} = \sum_{n,m} \sum_{i=1}^{S_{k,nm}} X_{i|k,nm}^{a,b}, \tag{9}$$

with $\mu_k^{a,b} = E\left[X_k^{a,b}\right] = \sum_{n,m} p_{a,b|nm,\text{Z}} S_{k,nm}$. Let $x_k^{a,b} = \left|\mathcal{Z}_k^{a,b}\right|$ denote the observed outcome of the random variable $X_k^{a,b}$ for a given trial. Then, if $\left(2\varepsilon_{a,b}^{-1}\right)^{1/\mu_{k,\text{L}}^{a,b}} \leq \exp\left[3/(4\sqrt{2})\right]^2$ and $\left(\hat{\varepsilon}_{a,b}^{-1}\right)^{1/\mu_{k,\text{L}}^{a,b}} < \exp(1/3)$, with

$$\mu_{k,\text{L}}^{a,b} = \left|\mathcal{Z}_k^{a,b}\right| - \sqrt{\sum_{a,b} \left|\mathcal{Z}_k^{a,b}\right| / 2 \ln\left(1/\epsilon_{a,b}\right)}, \tag{10}$$

the Claim above implies that

$$\left|\mathcal{Z}_k^{a,b}\right| = \sum_{n,m} p_{a,b|nm,\text{Z}} S_{k,nm} + \delta_{a,b}, \tag{11}$$

except with error probability $\gamma_{a,b} = \epsilon_{a,b} + \varepsilon_{a,b} + \hat{\varepsilon}_{a,b}$, where $\delta_{a,b} \in \left[-\Delta_{a,b}, \hat{\Delta}_{a,b}\right]$, with $\Delta_{a,b} = g\left(\left|\mathcal{Z}_k^{a,b}\right|, \varepsilon_{a,b}^4/16\right)$ and $\hat{\Delta}_{a,b} = g\left(\left|\mathcal{Z}_k^{a,b}\right|, \hat{\varepsilon}_{a,b}^{3/2}\right)$.

Using similar arguments, we find that the parameter $m_{k,0}$ can be written as

$$m_{k,0} = \sum_m p_{a_\text{s},b_\text{s}|0_m,\text{Z}} S_{k,0m} - \Delta_0, \tag{12}$$

except with error probability ε_0, where $\Delta_0 = g\left(\sum_m p_{a_\text{s},b_\text{s}|0_m,\text{Z}} S_{k,0_m}, \varepsilon_0\right)$.

Now it is easy to find a lower bound for $m_{k,0}$. One only needs to minimize equation (12) given the linear constraints imposed by equation (11) for all a, b. This problem can be solved either by using numerical tools as linear programming[46] or, for some particular cases, by using analytical techniques. See Supplementary Notes 1 and 2 for details.

The second step of the procedure is quite direct. Note that Alice forms her bit string Z_k using n_k random indexes from $\mathcal{Z}_k^{a_\text{s},b_\text{s}}$. Using ref. 51 we obtain

$$n_{k,0} = \max\left\{\left\lfloor n_k \frac{m_{k,0}}{\mid \mathcal{Z}_k^{a_\text{s},b_\text{s}} \mid} - n_k \Lambda(\mid \mathcal{Z}_k^{a_\text{s},b_\text{s}} \mid, n_k, \varepsilon_{k,0}'')\right\rfloor, 0\right\}, \tag{13}$$

except with error probability

$$\varepsilon_{k,0} \leq \varepsilon_{k,0}' + \varepsilon_{k,0}'', \tag{14}$$

where $\varepsilon_{k,0}'$ corresponds to the total error probability in the estimation of $m_{k,0}$, and the function $\Lambda(x, y, z)$ is defined as $\Lambda(x, y, z) = \sqrt{(x - y + 1)\ln(z^{-1})/(2xy)}$.

References

1. Gisin, N. *et al.* Quantum cryptography. *Rev. Mod. Phys.* **74,** 145–195 (2002).
2. Scarani, V. *et al.* The security of practical quantum key distribution. *Rev. Mod. Phys.* **81,** 1301–1350 (2009).
3. Qi, B. *et al.* Time-shift attack in practical quantum cryptosystems. *Quantum Inf. Comput.* **7,** 73–82 (2007).
4. Fung, C.-H. F. *et al.* Phase-remapping attack in practical quantum-key-distribution systems. *Phys. Rev. A* **75,** 032314 (2007).
5. Lamas-Linares, A. & Kurtsiefer, C. Breaking a quantum key distribution system through a timing side channel. *Opt. Express* **15,** 9388–9393 (2007).
6. Zhao, Y. *et al.* Quantum hacking: experimental demonstration of time-shift attack against practical quantum-key-distribution systems. *Phys. Rev. A* **78,** 042333 (2008).
7. Nauerth, S. *et al.* Information leakage via side channels in freespace BB84 quantum cryptography. *New J. Phys.* **11,** 065001 (2009).
8. Xu, F., Qi, B. & Lo, H.-K. Experimental demonstration of phase-remapping attack in a practical quantum key distribution system. *New J. Phys.* **12,** 113026 (2010).
9. Lydersen, L. *et al.* Hacking commercial quantum cryptography systems by tailored bright illumination. *Nat. Photon.* **4,** 686–689 (2010).
10. Gerhardt, I. *et al.* Full-field implementation of a perfect eavesdropper on a quantum cryptography system. *Nat. Commun.* **2,** 349 (2011).
11. Weier, H. *et al.* Quantum eavesdropping without interception: an attack exploiting the dead time of single-photon detectors. *New J. Phys.* **13,** 073024 (2011).
12. Mayers, D. & Yao, A. C.-C. in *Proc. of the 39th Annual Symposium on Foundations of Computer Science (FOCS98)* 503–509 (IEEE Computer Society, 1998).
13. Acín, A. *et al.* Device-independent security of quantum cryptography against collective attacks. *Phys. Rev. Lett.* **98,** 230501 (2007).
14. Pironio, S. *et al.* Device-independent quantum key distribution secure against collective attacks. *New J. Phys.* **11,** 045021 (2009).
15. McKague, M. Device independent quantum key distribution secure against coherent attacks with memoryless measurement devices. *New J. Phys.* **11,** 103037 (2009).
16. Masanes, L., Pironio, S. & Acín, A. Secure device-independent quantum key distribution with causally independent measurement devices. *Nat. Commun.* **2,** 238 (2011).
17. Barrett, J., Colbeck, R. & Kent, A. Memory attacks on device-independent quantum cryptography. *Phys. Rev. Lett.* **110,** 010503 (2013).
18. Bell, J. S. On the Einstein-Podolsky-Rosen paradox. *Physics* **1,** 195–200 (1964).

19. Clauser, J. F. *et al.* Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.* **23,** 880–884 (1969).
20. Pearle, P. Hidden-variable example based upon data rejection. *Phys. Rev. D* **2,** 1418–1425 (1970).
21. Gisin, N., Pironio, S. & Sangouard, N. Proposal for implementing device-independent quantum key distribution based on a heralded qubit amplifier. *Phys. Rev. Lett.* **105,** 070501 (2010).
22. Curty, M. & Moroder, T. Heralded-qubit amplifiers for practical device-independent quantum key distribution. *Phys. Rev. A* **84,** 010304(R) (2011).
23. Lo, H.-K., Curty, M. & Qi, B. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **108,** 130503 (2012).
24. Rubenok, A. *et al.* Real-world two-photon interference and proof-of-principle quantum key distribution immune to detector attacks. *Phys. Rev. Lett.* **111,** 130501 (2013).
25. Ferreira da Silva, T. *et al.* Proof-of-principle demonstration of measurement device independent QKD using polarization qubits. *Phys. Rev. A* **88,** 052303 (2013).
26. Liu, Y. *et al.* Experimental measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **111,** 130502 (2013).
27. Tang, Z. *et al.* Experimental demonstration of polarization encoding measurement-device-independent quantum key distribution. Preprint at (http://arxiv.org/abs/1306.6134) (2013).
28. Curty, M., Lewenstein, M. & Lütkenhaus, N. Entanglement as a precondition for secure quantum key distribution. *Phys. Rev. Lett.* **92,** 217903 (2004).
29. Lim, C. C. W. *et al.* Device-Independent quantum key distribution with local Bell test. *Phys. Rev. X* **3,** 031006 (2013).
30. Song, T.-T. *et al.* Finite-key analysis for measurement-device-independent quantum key distribution. *Phys. Rev. A* **86,** 022332 (2012).
31. Ma, X., Fung, C.-H. F. & Razavi, M. Statistical fluctuation analysis for measurement-device-independent quantum key distribution. *Phys. Rev. A* **86,** 052305 (2012).
32. Tomamichel, M., Lim, C. C. W., Gisin, N. & Renner, R. Tight finite-key analysis for quantum cryptography. *Nat. Commun.* **3,** 634 (2012).
33. Bacco, D., Canale, M., Laurenti, N., Vallone, G. & Villoresi, P. Experimental quantum key distribution with finite-key security analysis for noisy channels. *Nat. Commun.* **4,** 2363 (2013).
34. Lim, C. C. W., Curty, M., Walenta, N., Xu, F. & Zbinden, H. Concise security bounds for practical decoy-state quantum key distribution. *Phys. Rev. A* **89,** 022307 (2014).
35. Renner, R. *Security of Quantum Key Distribution*. PhD thesis, ETH Zurich (2005).
36. Müller-Quade, J. & Renner, R. Composability in quantum cryptography. *New J. Phys.* **11,** 085006 (2009).
37. Chernoff, H. A measure of asymptotic efficiency for tests of a hypothesis based on the sum of observations. *Ann. Math. Stat.* **23,** 493–507 (1952).
38. Hwang, W.-Y. Quantum key distribution with high loss: toward global secure communication. *Phys. Rev. Lett.* **91,** 057901 (2003).
39. Lo, H.-K., Ma, X. & Chen, K. Decoy state quantum key distribution. *Phys. Rev. Lett.* **94,** 230504 (2005).
40. Wang, X.-B. Beating the photon-number-splitting attack in practical quantum cryptography. *Phys. Rev. Lett.* **94,** 230503 (2005).
41. Bennett, C. H. & Brassard, G. in *Proc. IEEE Int. Conf. on Comp. Sys. and Signal Processing* 175–179 (Bangalore, India, 1984).
42. Biham, E., Huttner, B. & Mor, T. Quantum cryptographic network based on quantum memories. *Phys. Rev. A* **54,** 2651–2658 (1996).
43. Inamori, H. Security of practical time-reversed EPR quantum key distribution. *Algorithmica* **34,** 340–365 (2002).
44. Lütkenhaus, N. Estimates for practical quantum cryptography. *Phys. Rev. A* **59,** 3301–3319 (1999).
45. Azuma, K. Weighted sums of certain dependent random variables. *Tôhoku Math. J.* **19,** 357–367 (1967).
46. Vanderbei, R. J. (ed.) *Linear Programming: Foundations and Extensions*. International Series in Operations Research and Management Science, 3rd edn (Springer, 2008).
47. Ursin, R. *et al.* Entanglement-based quantum communication over 144 km. *Nat. Phys.* **3,** 481–486 (2007).
48. Xu, F. *et al.* Practical aspects of measurement-device-independent quantum key distribution. *New J. Phys.* **15,** 113007 (2013).
49. Hadfield, R. H. Single-photon detectors for optical quantum information applications. *Nat. Photon.* **3,** 696–705 (2009).
50. Marsili, F. *et al.* Detecting single infrared photons with 93% system efficiency. *Nat. Photon.* **7,** 210–214 (2013).
51. Serfling, R. J. Probability inequalities for the sum in sampling without replacement. *Ann. Statist.* **2,** 39–48 (1974).
52. Tomamichel, M., Colbeck, R. & Renner, R. Duality between smooth min- and max-entropies. *IEEE Trans. Inf. Theory* **54,** 4674–4681 (2010).
53. Vitanov, A., Dupuis, F., Tomamichel, M. & Renner, R. Chain rules for smooth min- and max-entropies. *IEEE Trans. Inf. Theory* **59,** 2603–2612 (2013).

Acknowledgements

We thank Xiongfeng Ma and Johan Löfberg for valuable comments and stimulating discussions, and Lina M. Eriksson for comments on the writing and presentation of the paper. F.X. thanks the Paul Biringer Graduate Scholarship for financial support. We acknowledge support from the European Regional Development Fund (ERDF), the Galician Regional Government (projects CN2012/279 and CN 2012/260, 'Consolidation of Research Units: AtlantTIC'), NSERC, the CRC program, the National Centre of Competence in Research QSIT, the Swiss NanoTera project QCRYPT, the FP7 Marie-Curie IAAP QCERT project and CHIST-ERA project DIQIP. K.T. acknowledges support from the project 'Secure photonic network technology' as part of 'The project UQCC' by the National Institute of Information and Communications Technology (NICT) of Japan, and from the Japan Society for the Promotion of Science (JSPS) through its Funding Program for World-Leading Innovative R&D on Science and Technology (FIRST Program).

Author contributions

All authors contributed extensively to the work presented in this paper.

Additional information

Supplementary Information accompanies this paper at http://www.nature.com/naturecommunications

Competing financial interests: The authors declare no competing financial interests.

Reprints and permission information is available online at http://npg.nature.com/reprintsandpermissions/

How to cite this article: Curty, M. *et al.* Finite-key analysis for measurement-device-independent quantum key distribution. *Nat. Commun.* 5:3732 doi: 10.1038/ncomms4732 (2014).