Supplemental Material

1. Detection

To detect the photons in a two-dimensional grid, we use an ICCD (Lambert HICAM 500S). It consists of an intensifier stage fiber-coupled to a CMOS camera of 1280×1024 pixels. The photocathode of the ICCD acts as a gate and is triggered by the herald photons at 280 kHz. The delay between the trigger signal and the signal photon was measured to be 91 ns. The gate width of the intensifier is 5 ns. The CMOS camera is read out with 500 frames per second. The variance of the read-out noise of the CMOS is 0.4 counts and a threshold of 5 counts is set to filter the readout noise from the data. Moreover, a threshold on the size and intensity of detection events is set to between 2 and 10 pixels and between 1 and 60 counts, respectively, to remove unwanted spurious ion events. This method is similar to [1, 2].

2. Trojan-horse attacks

The quantum channel connecting Alice and Bob could be used as a door by an eavesdropper to read out the state of Alice's and Bob's devices, making the setup vulnerable against Trojan-horse attacks [3]. To counteract such attacks, the optical devices should only be active when the photons are sent. In our setup that could be realized by replacing the mechanical switch of the half-wave plate with a fast electro-optic modulator and the liquid-crystal SLM by a faster digital micromirror device. They could be synchronized to the photon arrival. Another countermeasure is to use bandpass filters and optical isolators at the entrance of Alice's device. Alice should also use auxiliary detectors to detect any light entering her device to detect attacks. In the finite-key regime the security of leaky decoy-state BB84 has been investigated [4].

3. Intercept-resend attack

In this attack, Eve intercepts a fraction η of the quantum states and performs projective measurements randomly choosing one of the two mutually unbiased bases. Eve resends her measurement result, introducing an error due to the collapse of the wavefunction. For the security of the protocol, we need to ensure that the information Eve can gain from intercepting the communication is lower than the mutual information between sender and receiver [5, 6]. Assuming an intercept-resend attack, the information Eve can learn is $I(\text{Eve}) = \frac{\eta}{2} I(\text{Alice})$ with η the fraction of intercepted photons and $I(\text{Alice})$ the sent information of Alice. Averaged over the compatible bases, we find $I(\text{Alice}) = 9.4$ bit. An eavesdropper can extract a maximum of $I(\text{Eve}) = \eta 5.72$ bit. Therefore, just as in the

case of the original BB84, information gain is only possible at the expense of disturbing the signal [7]. An eavesdropper will be recognized in postprocessing, since she collapses the wavefunction and thereby increases the error rate of the key generated by Alice and Bob. Alice and Bob will have to compare a random part of their key to decide if they have been eavesdropped. Intercepting a fraction of η photons, an attacker introduces an error of

$$E_{\mathrm{Eve}} = \frac{\eta}{2}\frac{d-1}{d}, \tag{1}$$

where d is the number of symbols. To calculate the quantum bit error rate of the sifted key, we used the Gray code [8] to encode the x and y position of the symbol in a bit string. In this way, we reduce the bit error rate, since 31.3% of the error is due to crosstalk to neighboring symbols. In the Gray code, neighboring symbols have a minimum hamming distance of 1. We calculated the averaged quantum bit error rate over all symbols to be $Q_{\mathrm{II}} = 0.078$ with a standard deviation of $\Delta Q_{\mathrm{II}} = 0.042$ for II configuration and $Q_{\mathrm{FF}} = 0.074$ and $\Delta Q_{\mathrm{FF}} = 0.029$ for FF configuration. We assume Alice and Bob set their threshold to detect eavesdropping to a bit error rate of $Q + \sigma$, where Q is the averaged quantum bit error rate. In this case Eve could only intercept a fraction η of the photons.

4. Basis guess fidelity

In practical QKD, Alice's basis choice could leak to an eavesdropper via side channels or imperfect encoding. To include this into the model, we added a guess fidelity of ϵ. Eve can not guess the basis if $\epsilon = 0$, while $\epsilon = 1$ means that Eve knows Alice's basis choice. In our experiment, we measured $\epsilon \sim 0.15$ by a correlation measurement performed with classical light. Eve can then extract the information

$$I(\mathrm{Eve}) = \frac{\eta}{2}\,(1+\epsilon)\,I(\mathrm{Alice}) \tag{2}$$

from what Alice sends. Thereby she adds an additional error of

$$Q_{\mathrm{Eve}} = \frac{1}{2}\,(1-\epsilon)\,\frac{d-1}{d}. \tag{3}$$

To detect eavesdropping, Alice and Bob must set an error threshold σ. The error rate introduced by Eve's perturbation of the quantum channel has to be lower than this threshold to stay unnoticed. The quantum bit error rate including an eavesdropper is

$$Q_{\mathrm{Total}} = (1-\eta)Q + \eta\,(Q + (1-Q)Q_{\mathrm{Eve}}) \tag{4}$$

$$= Q + (1-Q)\eta Q_{\mathrm{Eve}}. \tag{5}$$

From the relation

$$Q_{\mathrm{Total}} \leq Q + \sigma, \tag{6}$$

the maximum fraction of intercepted photons is

$$\eta_{\max} = \frac{\sigma}{(1-Q)Q_{\mathrm{Eve}}}, \tag{7}$$

which depends on the fidelity to guess the correct basis ϵ and the threshold σ. The minimum fidelity between Alice and Bob reduces from F to

$$F_{\text{Total}} = F\left(1 - \eta Q_{\text{Eve}}\right). \tag{8}$$

Now it is possible to calculate the distance of information between Bob and Eve, which is a measure for the secure key rate. The information distance is defined as

$$\delta = I_{\text{AB}} - I(\text{Eve}). \tag{9}$$

The amount of information Bob receives depends on the amount of information Alice transmits and on the channel noise. Therefore

$$I(\text{Bob}) = Q_{\text{Total}} I(\text{Alice}). \tag{10}$$

Combining equation 2 and 10, the information distance can be written as

$$\delta = \left[(1 - Q_{\text{Total}}) - \frac{\eta}{2}(1 + \epsilon)\right] I(\text{Alice}). \tag{11}$$

By substituting $\eta_{\max}$ from equation 7 to this expression, the minimum information distance can be plotted as a function of ϵ and σ in figure 1. Compared to equation (5) in the main article the prefactor n/N does not appear, since already a small fraction of the key is enough for parameter estimation. Moreover, the error correction and parameter estimation as well as the uncertainties about Eve's entropies lower the secret fraction.

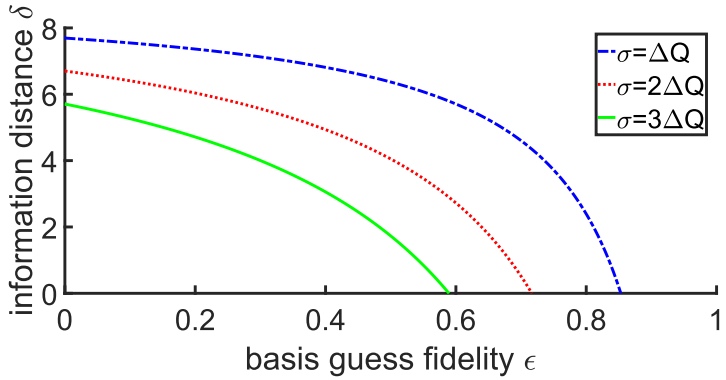

Figure 1. The minimum secret information distance δ against the basis guess fidelity ϵ for three different thresholds σ.

The information distance δ grows monotonically with decreasing threshold σ, but becomes smaller with increasing ϵ, as visible in Fig. 1. If Eve knows Alice's basis choice ($\epsilon = 1$), her measurements will no longer add noise, which allows here to intercept the quantum communication without being detected. In comparison to the finite-key-length secret fraction in the case of collective attacks, the values the minimum secret information δ is larger.

[1] Morris P A, Aspden R S, Bell J E C, Boyd R W and Padgett M J 2015 *Nature Communications* **6** 1–6 ISSN 2041-1723
[2] Aspden, R S and Tasca, D S and Boyd, R W and Padgett, M J 2013 *New Journal of Physics* **15** 073032
[3] Gisin N, Fasel S, Kraus B, Zbinden H and Ribordy G 2006 *Phys. Rev. A* **73** 022320
[4] Wang W, Tamaki K and Curty M 2018 *New J. Phys.* **20** 083027
[5] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145
[6] Scarani V, Bechmann-Pasquinucci H, Cerf N J, Dušek M, Lütkenhaus N and Peev M 2009 *Rev. Mod. Phys.* **81** 1301
[7] Nielsen M A and Chuang I 2002 Quantum computation and quantum information
[8] Gray F 1953 Pulse code communication, us patent 2,632,058