Supplementary material to Entanglement-based quantum key distribution with a blinking-free quantum dot operated at a temperature up to 20 K

Christian Schimpf[a,*], **Santanu Manna**[a,*], **Saimon F. Covre da Silva**[a], **Maximilian Aigner**[a], **Armando Rastelli**[a]

[a]Institute of Semiconductor and Solid State Physics, Johannes Kepler University, Altenbergerstraße 69, 4040 Linz, Austria

*Christian Schimpf, christian.schimpf@jku.at

*Santanu Manna, santanu.manna@jku.at

*These authors contributed equally.

1 Details the sample fabrication and properties

1.1 Sample growth

Step no.		Description	Material	Thickness (nm)	Growth interruption time (sec)	Substrate temperature by thermo-couple (°C)	Pressure (mbar)	Arsenic aperture (mm)
1			GaAs buffer*	378		620	1.50E-6	7
2			GaAs buffer	12		676	1.90E-6	7
3			Al0.95Ga0.05As	65.15		676	2.0E-6	7
4	No. of Loops 6	DBR Loop 1.1	Al0.20Ga0.80As	56.56		676	2.04E-6	7
5		DBR Loop 1.2	Al0.95Ga0.05As	65.15		676	2.08E-6	7
6		DBR Loop 1.3	GI	0	30	676	2.35E-6	7
7			GI	0	180	ramp down to 620	1.58E-6	7
8		Spacer	Al0.15Ga0.85As	95		620	2.03E-6	7
9			GI	0	120	ramp down to 580	2.32E-6	
10		n-doped ~1.0E+18/cc	Al0.15Ga0.85As	95		580	1.89E-6	7
11		Si seggregation preventing layer	Al0.15Ga0.85As	5		580	1.80E-6	7
12			GI	0	70	ramp up to 620	2.17E-6	7
13			Al0.15Ga0.85As	10		620	1.92E-6	7
14			GI	0	120	620	2.17E-6	7
15		Barrier	Al0.33Ga0.67As	15		620	1.83E-6	7
16			GI (Close As)	0	10	620		0
17			Al	0.13		620		0
18			GI	0	20	620	1.90E-7	0
19		Etching	GI	0	60	620	2.34E-7	0.62
20		Etching	GI	0	60	620	2.66E-7	0.64
21		Crystallization	GI	0	60	620	2.09E-6	7
22		Filling	GaAs	1.9		620	2.03E-6	7
23			GI	0	45	620	2.27E-6	7
24		Barrier	Al0.33Ga0.67As	268		620	1.74E-6	7
25			GI	0	300	ramp down to 570	2.43E-6	7
26		p+ doped ~5E+18/cc	Al0.15Ga0.85As	65	C	570	2.00E-6	7
27			GI	0	40	570	1.90E-6	7
28		p++ doped ~1E+19/cc	Al0.15Ga0.85As	5	C	570	1.92E-6	7
29		p++ doped cap ~1E+19/cc	GaAs	10	C	570	1.95E-6	7

Fig S1 Growth protocol of the investigated charge tunable diode structure containing GaAs dots grown by molecular beam epitaxy.

The investigated charge tunable diode structure containing GaAs dots was grown by molecular beam epitaxy. The growth protocol of this structure is depicted in Fig. S1. "GI" refers to a growth interruption. The (*) refers to a GaAs buffer growth rate which was different from other GaAs layers in the protocol. The growth rate it is given in the table below (with the same symbol). Deoxidation temperature of the GaAs wafer is found to be $591\ ^{\circ}\mathrm{C}$ using a thermocouple.

Table S1 Growth rate for different compounds

Material	Growth rate (µm/h)
GaAs	0.300
GaAs buffer*	0.400
Al0.15Ga0.85As	0.353
Al0.20Ga0.80As	0.375
Al0.33Ga0.67As	0.448
Al0.95Ga0.05As	0.402

Table S2 Beam equivalent pressure for the used Arsenic valve apertures

Valve Aperture (mm)	Beam equivalent pressure (mbar)
0.62	1.74E-6
0.64	1.92E-6
7.0 (completely open)	3.32E-5

1.2 Device fabrication

After growth of the p-i-n diode structure, fabrication is carried out to make electrical contacts to enable electric field variation and thus the charge tuning. Different steps involved in this fabrication can be seen Fig. S2.

The electrical contacts to the n- and p-doped layer are established by optical lithography, non-selective wet etching, metal deposition and thermal treatment. First, an optical lithography step is done to expose the portion of the sample for wet etching. This etching is performed such that it

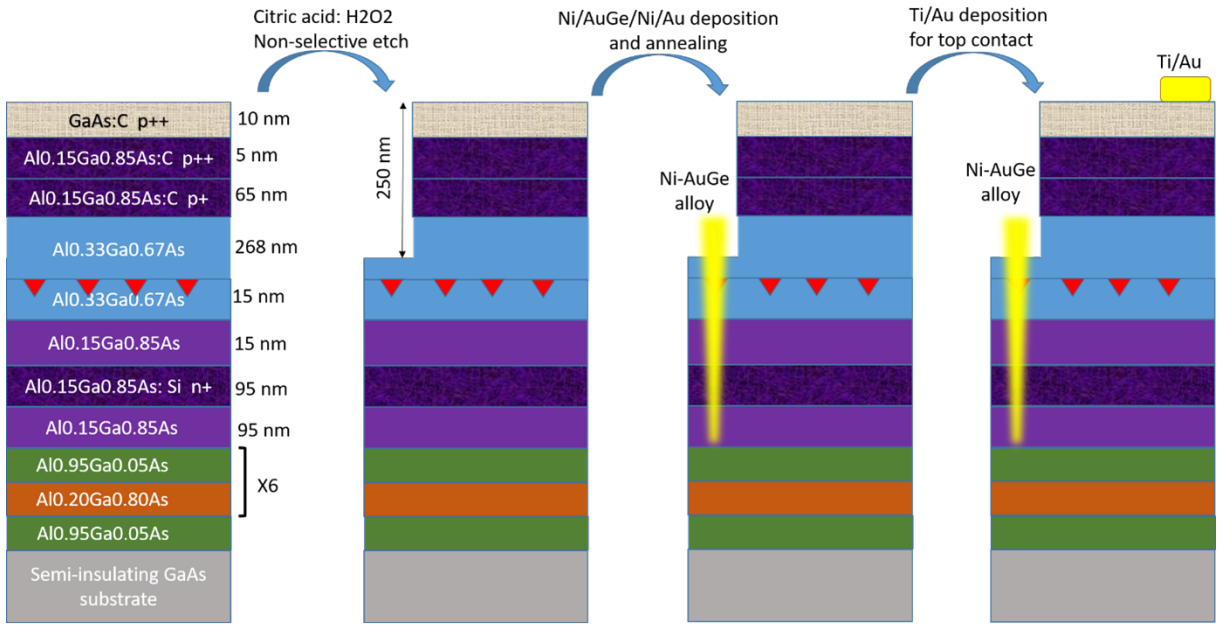

Fig S2 Fabrication steps for a charge tunable diode: Pristine sample structure to the fabricated contacts for the n- and p- sides using lithography, non-selective wet etching, metal deposition and thermal treatment.

stops inside the undoped $Al_{0.33}Ga_{0.67}As$ layer on the top of the QD layer. The chemical etching is done using citric acid solution ($12.5\,\mathrm{g}$ citric acid powder plus $12.5\,\mathrm{g}$ water) with H_2O_2 ($1\,\mathrm{ml}$) with an etching rate of about $1.9\,\mathrm{nm/s}$. This wet etching is non-selective and here we remove $250\,\mathrm{nm}$ material in 131 sec. On the exposed layer a Ni/AuGe/Ni/Au ($10/150/40/100\,\mathrm{nm}$) contact is deposited by a combination of thermal and e-beam evaporation and annealed at $420\,^{\circ}\mathrm{C}$ for $2\,\mathrm{min}$ in Ar+H_2 environment to make Ni-AuGe alloy and diffuse the contact down to the n-doped layer. A Ti/Au layer ($10/100\,\mathrm{nm}$), deposited on the uppermost p-layer after a lithography step, forms the second contact. Before deposition of this Ti/Au layer, a dip in HCl:H_2O=1:1 for $30\,\mathrm{sec}$ is useful to remove native oxide. For increasing the collection efficiency a Zirconia solid-immersion-lens (SIL) is placed on top of the sample surface.

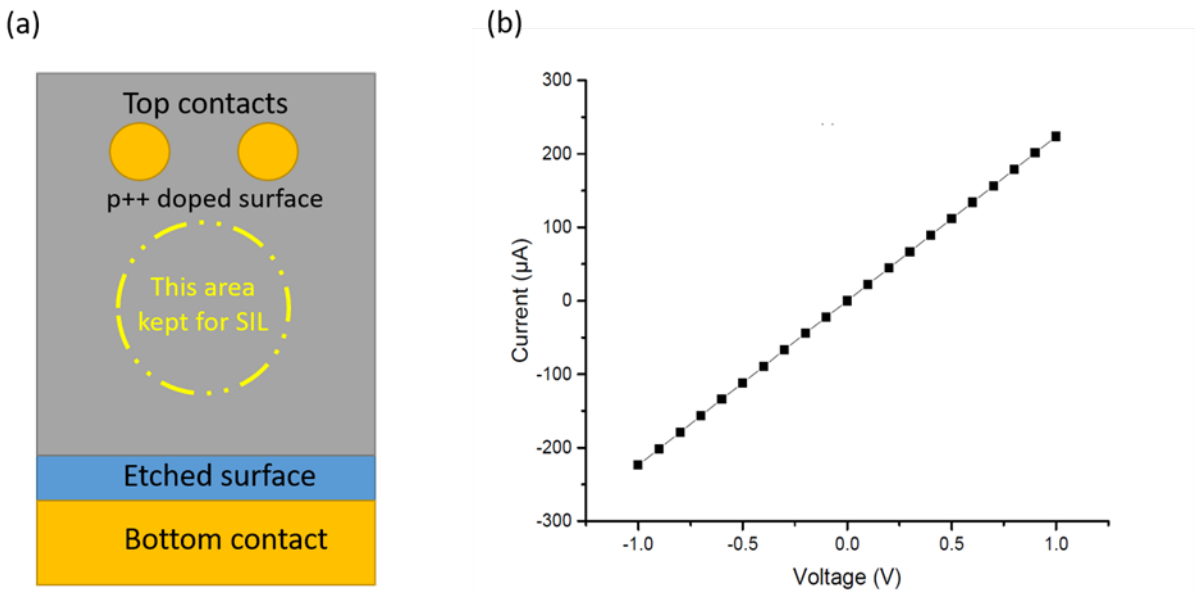

Fig S3 (a) Top view of the fabricated p-i-n diode. (b) I-V trace for the two top contacts on the p++ doped surface showing Ohmic behavior at $5.4\,\mathrm{K}$.

1.3 Electrical and optical properties

1.3.1 Ohmic behaviour of p-contact

The Ohmic behavior of the p-contact is verified using a simple current-voltage (I-V) trace for two circular contacts separated by $1\,\mathrm{mm}$ on top p++ doped surface, see Figs. S3(a-b). It's important that the contacts are deposited after a short dip in a diluted HCl solution (HCl:H_2O=1:1), otherwise the contact might show a non-linear I-V trace or linear trace with comparably high resistance.

1.3.2 I-V trace for the p-i-n diode

I-V trace of the charge tunable p-i-n diode containing GaAs QDs has been measured at dark condition at $5.4\,\mathrm{K}$ (see Fig. S4), which shows rectification behavior with a knee-voltage of $0.86\,\mathrm{V}$.

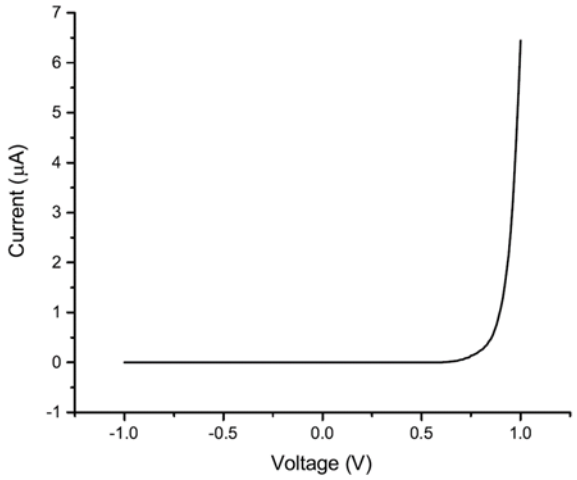

Fig S4 I-V trace for the charge tunable p-i-n diode showing rectification behavior at a temperature of $5.4\,\mathrm{K}$.

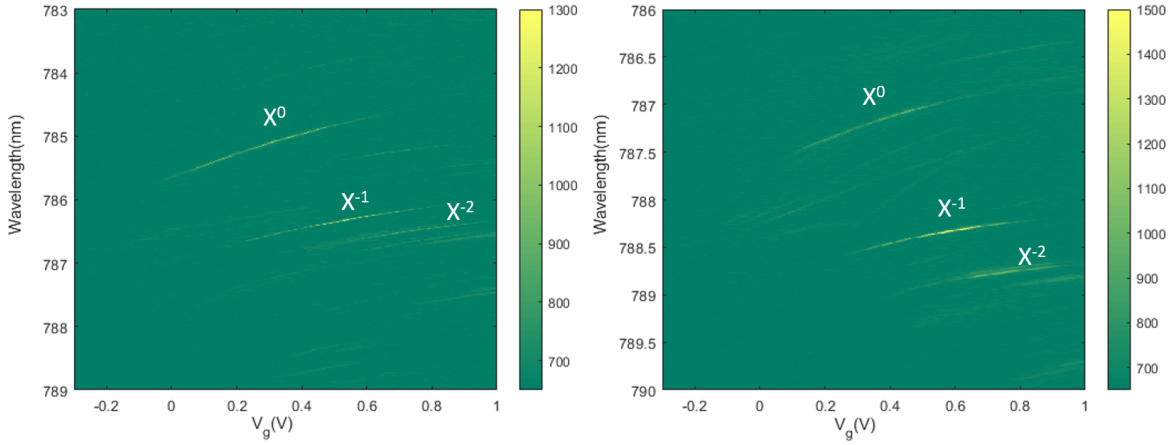

Fig S5 Charge plateaus for two different QDs at a temperature of $6\,\mathrm{K}$ while this QD is being excited by a non-resonant $632.8\,\mathrm{nm}$ laser.

1.3.3 Charging behaviour

The advantage of a charge tunable diode is the ability to charge a QD by electrons sequentially by applying more and more positive gate voltage (V_g) with respect to the n-contact. The resulting charge plateaus can be observed by photoluminescence mapping as a funtion of the gate voltage. Figure S5 represents such charge plateau characteristics for two different GaAs QDs excited by a non-resonant He-Ne laser with a wavelength of $632.8\,\mathrm{nm}$. In this case we can see several plateaus,

some of them denoted as X^0, X^{-1} and X^{-2}.

2 Complementary data

2.1 Decay dynamics at a temperature of 5 K

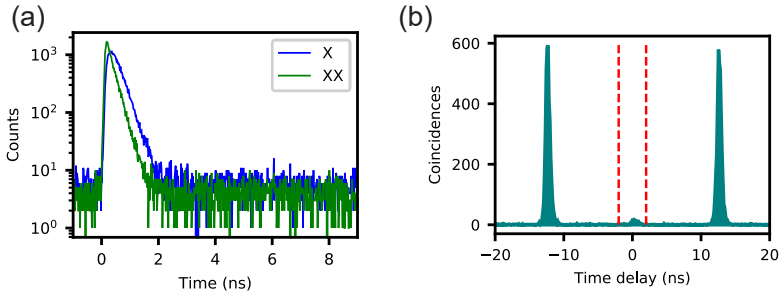

Fig S6 Decay dynamics of a QD in a p-i-n diode structure at a temperature of 5 K under resonant two-photon-excitation. (a) Lifetime trace of the XX and X photons, with lifetimes of 116(2) ps and 238(3) ps, respectively. (b) Example of a coincidence histogram between the XX and X photons in the HV measurement basis. The red dashed lines indicate the time-bin of 2 ns in which the coincidences are summed up to calculate the peak areas.

2.2 Dependence of the QBER on the correlation histogram time-bin

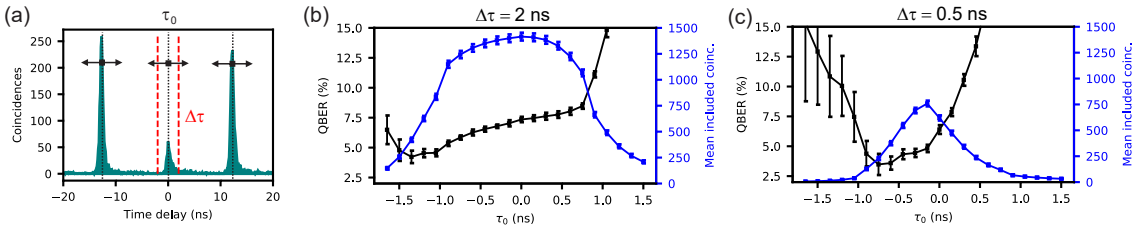

Fig S7 Dependency of the QBER on the correlation histogram time-bin. (a) Example histogram for a correlation measurement between the XX and X photons projected into the bases H and V, respectively, used for determining the 2-qubit density matrix in polarization space ρ. The coincidences are summed up within a time-bin of $\Delta\tau$ around a center time delay τ_0. The side-peaks are then considered to be at integer multiples of 12.5 ns (the excitation laser repetition period). (b) Expected QBER (black) calculated from ρ in polarization space and the mean number of coincidences (blue) lying within $\Delta\tau = 2$ ns (as used during key generation) as a function of τ_0. (c) Same situation as in (b), but with $\Delta\tau = 0.5$ ns.

Figure S7(a) depicts a typical correlation histogram (here: in the HV basis), as used for the most likelihood estimation of the 2-qubit density matrix in polarization space ρ (see section 3.2). The

coincidences are summed up within the time-bin $\Delta\tau = 2\,\mathrm{ns}$ around the time delay $\tau_0 = 0$, which are the values used in this work for both calculating ρ (see Fig. 2 in the main text) and for the key generation process. The side-peaks are then assumed to be located at $\tau_0 + z\,T_\mathrm{R}$ (with $T_\mathrm{R} = 12.5\,\mathrm{ns}$ the laser repetition rate and $z \in \mathcal{Z}\backslash 0$). Figure S7(b) shows the expected QBER calculated from ρ (with Eq. (1) in the main text), when varying τ_0 at a fixed time-bin of $\Delta\tau = 2\,\mathrm{ns}$, and the mean number of coincidences lying withing $\Delta\tau$ (averaged overall coincidence histograms). For $\tau_0 = 0$ the value of $7.5\,\%$ emerges, which corresponds to the QBEr estimation in the main text. For $\tau_0 > 0$ the expected QBER rises monotonically, as more photons from the slow X decay channel contribute to the coincidences. For $\tau_0 < 0$ the expected QBER initially drops to about $4.6\,\%$, where a minimum of the slow X decay channel contributes to the coincidence statistics. For even lower τ_0, coincidences from the previous side-peak get included into the time-bin, leading to a rising QBER again, and the error rises due to the low overall coincidence number. Figure S7(c) shows the same situation, but with $\Delta\tau = 0.5\,\mathrm{ns}$. Here, the number of included coincidences is inherently limited, but even lower expected QBER values can be reached.

These findings highlight that the choice of τ_0 and $\Delta\tau$ during the key generation process matter. In this work, τ_0 is found by tracking the maximum of the peak corresponding to the correlated XX and X photons, which effectively maximizes the raw key rate, but is not necessarily the best choice for a low QBER, as evident from Figs. S7(b-c).

3 Details to measurement data processing

3.1 Pair-emission probability

For an unpolarized pair of photons from the same decay cascade the coincidence rate scales linearly with the pair-emission probability ϵ, while the coincidence rate between different excitation cycles

scales with ϵ^2. Comparing the number of events in the unpolarized cross-correlation histogram (Fig. 2(e) in the main text) at $\tau = 0$ with the average of the events at different τ therefore allows to deduce ϵ, according to the following equation:

$$\frac{A_0}{\langle A_S \rangle} = \frac{n_0}{n_S} = \frac{1}{\epsilon}, \tag{1}$$

where A_0 is the area of the middle peak of the correlation histogram and $\langle A_S \rangle$ is the average side peak area.

3.2 Polarization density matrix estimation

For measuring the density matrix of the two-qubit state of the emitted photon pair in polarization space $\mathcal{H}^2 \otimes \mathcal{H}^2$, we perform a full-state tomography by projecting the photon pairs on all 36 possible bi-local measurement bases formed by the permutations of $|b_1\rangle \otimes |b_2\rangle$, with $b_1, b_2 \in \{H, V, D, A, R, L\}$ (as defined in Ref. (*33*)). For each basis configuration, a cross-correlation measurement between the X and XX photons is performed. From these measurements, 36 measurement outcomes $n_\nu, \nu \in [1, 36]$ are extracted, corresponding to the middle-peak area within the red dashed lines indicated in Fig. 2(d) of the main text. These outcomes are then used in a most likelihood function as described in Ref. (*33*) Eq. (4.10):

$$\mathcal{L}(\mathbf{t}) = \sum_{\nu=1}^{36} \frac{[\hat{n}_\nu - n_\nu]^2}{2\,\hat{n}_\nu} \tag{2}$$

with

$$\hat{n}_\nu = \mathcal{N} \langle \psi_\nu | \hat{\rho}_p(\mathbf{t}) | \psi_\nu \rangle \tag{3}$$

being the predicted measurement outcome for the measurement basis vectors $|\psi_\nu\rangle$ and the model density matrix $\hat{\rho}_p$. The target is to vary $\mathtt{t}$ in order to minimize $\mathcal{L}$. At this point, we make two modifications in order to increase the accuracy of the estimator in the context of entangled photon-pairs from QDs .

The different basis configurations for the individual photons are established by rotating a half-wave-plate (HWP) and a quarter-wave-plate (QWP) in front of a polarizer, which defines the H basis. For example, the L basis is set by rotating the fast axis of the the HWP (QWP) to $\theta_H = 22.5°$ ($\theta_Q = 90°$) w.r.t. the easy axis of the polarizer. In reality, the retardances δ_H and δ_Q of the HWP and the QWP, respectively, are not exactly $\lambda/2$ and $\lambda/4$. We use the manufacturer's (Thorlabs) specifications, given as $\delta_H = 0.516\lambda$ and $\delta_Q = 0.258\lambda$, with $\lambda = 780\,\mathrm{nm}$. The single-qubit measurement basis formed by the QWP, HWP and polarizer is then given by

$$|b\rangle = G(\delta_Q, \theta_Q) G(\delta_H, \theta_H) \, |H\rangle \,, \tag{4}$$

with $G(\delta, \theta)$ being the transformation exerted by a general retarder with retardance δ and rotation angle θ w.r.t to H. The two-qubit basis vectors $|\psi_\nu\rangle$ in Eq. 3 are then the Dirac product of two single-qubit bases set for projecting the XX and X photons, respectively:

$$|\psi_\nu\rangle = |b_\nu^{\mathrm{X}}\rangle \otimes |b_\nu^{XX}\rangle \tag{5}$$

The second change reconsiders the normalization factor $\mathcal{N}$ in Eq. (3). In the original form as given in Ref. (*33*), the number of measured copies is assumed to be constant for all bases, which is difficult to guarantee in most experimental settings. Therefore, in order to make more accurate

prediction of $\hat{n}_\nu$, we introduce individual normalization factors for each measurement, so that

$$\mathcal{N} \to \mathcal{N}_\nu = n_\nu^{\mathrm{S}} \sum_j \frac{n_j}{n_j^{\mathrm{S}}},\ j \in \{\mathrm{HH,HV,VH,VV}\} \tag{6}$$

with n^{S} being the average side-peak area within a defined time-bin extracted from the cross-correlation histograms (example for the HV basis is shown in Fig. S6). By this adaption, the effect of count-rate variations over the full time span of the tomography is alleviated and also the non-unity XX preparation fidelity is accounted for.

4 Details to key generation and post-processing

4.1 Security analysis

The goal of the security analysis of a QKD is to ensure that a negligible amount of useful information about the shared key is available to a potential eavesdropper. This requires an accurate estimation of the possible information leaked to the public channel during the key generation and the error correction phases. To this end we adopt the security analysis as used in Ref. (*35*), which properly takes into account the uncertainty in the estimation of the QBER from a key with a finite length.

During the key generation phase a total of $m = 888082$ key bits were generated, where a fraction of $\beta = 0.1$ was used for estimating the QBER to $\delta = 0.842$, leaving the total raw key of length $n = m\,(1-\beta) = 807348$ bits stated in the main text. From these experimental parameters we need to extract the key length $l = \alpha\, n$, with α being the reconciliation efficiency, so that the total error probability (i.e. the probability to underestimate the QBER or to insufficiently compress the key) remains below a fixed security parameter $\epsilon_{\mathrm{QKD}} < 10^{-s}$. The choice of the security level

s is non-trivial and still up to debate. We set the target security level as $s = 9$, which is currently considered to yield a vanishing error probability.

The key error correction scheme assumed is based on Hamming codes, where the information leakage to the public channel during the correction step, which we need to compensate for, is given by $r = f_{\mathrm{EC}}\, h_2(\delta)\, n$ bits (with h_2 being the binary entropy function). The quantity $f_{\mathrm{EC}} = 1.19$ is an empirical value corresponding to the efficiency of the error correction process. A value greater than one means that a factor of f_{EC} of redundant information has to be sent over the public channel in order to successfully correct all errors (see Ref.(*39*) for an excellent explanation). For most error corrections schemes in the literature f_{EC} varies only little for rising δ (*39,40*), so we choose the same value of 1.19 as Ref. (*35*) and a hash key of length $t = 32$ used to check if the error correction succeeded.

With the parameters $m, \beta, n, \delta, r, t$ and s in place, we solve the optimization problem described on page 4 of Ref. (*35*) by varying the parameters ν and ζ to maximize the remaining key length l. We found a maximum key length of $l = 20649$, corresponding to a key reconciliation efficiency of $\alpha \approx 0.026$. We summarize the output set of floating point variables in Table S3 below (with 8 digits precision).

Table S3 Summarized parameter set for optimizing the key length l

ν	0.0179307
ζ	0.0162997
α	0.0255775