Demonstration of free-space reference frame independent quantum key distribution

J Wabnig\textsuperscript{1,3}, D Bitauld\textsuperscript{1}, H W Li\textsuperscript{1}, A Laing\textsuperscript{2}, J L O’Brien\textsuperscript{2} and A O Niskanen\textsuperscript{1}

\textsuperscript{1}Nokia Research Center, Broers Building, 21 J J Thomson Avenue, Cambridge CB3 0FA, UK
\textsuperscript{2}Centre for Quantum Photonics, H H Wills Physics Laboratory & Department of Electrical and Electronic Engineering, University of Bristol, Bristol BS8 1UB, UK
E-mail: joachim.wabnig@nokia.com

New Journal of Physics 15 (2013) 073001 (17pp)
Received 5 March 2013
Published 2 July 2013
Online at http://www.njp.org/
doi:10.1088/1367-2630/15/7/073001

Abstract. Quantum key distribution (QKD) is moving from research laboratories towards applications. As computing becomes more mobile, cashless as well as cardless payment solutions are introduced. A possible route to increase the security of wireless communications is to incorporate QKD in a mobile device. Handheld devices present a particular challenge as the orientation and the phase of a qubit will depend on device motion. This problem is addressed by the reference frame independent (RFI) QKD scheme. The scheme tolerates an unknown phase between logical states that vary slowly compared to the rate of particle repetition. Here we experimentally demonstrate the feasibility of RFI QKD over a free-space link in a prepare and measure scheme using polarization encoding. We extend the security analysis of the RFI QKD scheme to be able to deal with uncalibrated devices and a finite number of measurements. Together these advances are an important step towards mass production of handheld QKD devices.

\textsuperscript{3}Author to whom any correspondence should be addressed.

Content from this work may be used under the terms of the Creative Commons Attribution 3.0 licence. Any further distribution of this work must maintain attribution to the author(s) and the title of the work, journal citation and DOI.
## Contents

1. Introduction .......................... 2  
2. Experimental setup .................. 3  
3. Secure key fraction .................. 6  
4. Results and discussion .............. 8  
Appendix A. Keyrate for BB84 .......... 10  
Appendix B. Reference frame independent quantum key distribution ............. 11  
Appendix C. Conditional entropy decreases under projective measurement ........ 11  
Appendix D. Simplified density matrices for parameter estimation ............... 13  
Appendix E. Device model ................ 14  
Appendix F. Detector counts and correlation functions ......................... 15  
References ................................ 15

### 1. Introduction

Quantum key distribution (QKD) promises secure communications based not on the hardness of a mathematical problem but on the laws of physics [1–3]. The main effort in the development of QKD is directed towards long-range communication, mostly fibre-based [4–9] as well as in free space [10–13]. A prospective new application of QKD is in securing short-range line-of-sight communications between a terminal and a handheld device (see figure 1(a)) [14, 15]. Current mobile payment techniques, e.g. near field communications, have a range of security challenges including eavesdropping. Similar considerations apply to securing Wi-Fi access points. We believe that future handheld QKD systems can address these security challenges and provide a high degree of wireless security.

One of the unique problems faced by handheld QKD is the fact that the relative orientation of the emitter and the receiver is variable. In previous works, this problem has been addressed by using entanglement [16, 17] or by encoding information on angular momenta [18], which are invariant under rotation. The reference frame independent (RFI) QKD scheme proposed in [19] does not require entanglement and allows the use of polarization encoding without the need for alignment of the qubit reference frames. In this scheme the qubits are prepared and measured in three mutually unbiased bases. Only one of those bases, on which the key is encrypted, needs to be stable. The two other bases are allowed to drift slowly and are used to estimate the security parameters of the quantum channels. The requirement for one basis to be stable is met in most practical implementations. In the case of free-space polarization-based encoding, the stable basis is the circular polarization, which is rotation independent. Figure 1(b) shows the bases used by the emitter (Alice) $X_A, Y_A, Z_A$ and the receiver (Bob) $X_B, Y_B, Z_B$ for an undetermined relative orientation. The use of additional bases compared to e.g. BB84 enables the reference frame independence of the scheme.

In order to demonstrate the feasibility of such a protocol we implement a prepare and measure scheme based on faint pulses and analyse the security of the channel. In addition to the reference frame independence implied by the protocol, we develop a theoretical analysis that allows us to take into account deviations from the ideal perpendicular preparation and measurement bases. Although we cannot claim to achieve full device independence [20], which
Figure 1. (a) A mobile QKD terminal communicating with a stationary QKD terminal. The mobile terminal is free to rotate. (b) Poincaré sphere representation of Alice and Bob’s reference frames. The Z basis (circular polarization), represented by black vectors, is shared by Alice and Bob and is used as the key basis. Alice’s X and Y bases (horizontal/vertical and diagonal/antidiagonal), represented by red vectors, are aligned with the Poincaré sphere’s axes. Bob’s X and Y bases, represented in blue, are rotated with respect to Alice’s. A rotation of the terminal by the angle $\phi$ results in a rotation on the Poincaré sphere by $2\phi$.

generally requires entanglement, we are able to deal with device imperfections and uncalibrated devices within our selected model. In any QKD scheme the number of measurements available for the parameter estimation step is finite. Parameters obtained from the measurements are estimates with a non-zero variance, which impacts the secure key fraction as discussed in [21–23]. In our security analysis we take this into account to derive a secret key fraction. In this paper, section 2 describes the experimental setup we used to implement an RFI protocol, while in section 3 we analyse the security of the quantum channel including the influence of finite size effects, imperfectly calibrated devices and mismatched detector efficiencies. In section 4 we discuss our results.

2. Experimental setup

In the prepare and measure RFI protocol, Alice needs to be able to randomly pick a light polarization state out of three different bases, i.e. horizontal/vertical, antidiagonal/diagonal, left circular/right circular, corresponding to $X$, $Y$ and $Z$ basis. This is implemented by activating one of six 850 nm vertical-cavity surface-emitting laser (VCSEL) diodes. Their respective polarizations are separately engineered before their optical beams are combined in a common mode. They are electrically driven by a pattern generator with six individually controllable outputs. Each output generates 0.5 ns pulses and their amplitudes are adjusted so that the average photon number per pulse at Alice’s output is the same for all the lasers. Pseudorandom bit sequences allowing only one of the six lasers to be active every 4 ns (i.e. $250 \times 10^6$ pulses s$^{-1}$) are programmed in the pattern generator’s memory. The random bit pattern is repeated every 500 pulses. Engineering of the polarizations is performed by a set of polarizing beam splitters (PBSs) and waveplates (see figure 2). At first, the polarization of the VCSELs is ill-defined but it is filtered by the polarization beam splitters with an extinction ratio of about 13 dB. The outputs of the PBSs are polarized either horizontally or vertically depending on which laser is active. One of the PBS output’s polarization is left unchanged. The output of another PBS
Figure 2. Experimental implementation of RFI QKD with the layout of the emitter (Alice’s device) and the receiver (Bob’s device). Both Alice and Bob’s devices are mounted on a 10 cm × 10 cm metal plate and the distance between the two is slightly above 1 m. The compactness of our assembly can be seen in the insets.

passes through a 22.5° rotated λ/2 waveplate resulting in diagonal/antidiagonal polarizations. The output of the last PBS is directed towards a 45° rotated λ/4 waveplate resulting in left/right circular polarizations. The waveplate used in this experiment is achromatic but we estimate their retardance at 850 nm to be 0.535 and 0.265 (±0.05) for the half and quarter waveplates respectively. Those discrepancies together with the PBS extinction ratio are responsible for the biasing of the bases that are discussed in the theoretical section. After preparing the polarizations the three resulting beams are combined with two non-PBSs. The spatial profile of the combined beams is filtered with a 1 mm pinhole, while the direction profiles are filtered with a 5 μm pinhole between two lenses. Finally, light passes through a neutral density filter reducing the intensity down to below 0.05 photons per pulse. After the output of the emitter, a rotating λ/2 waveplate is used to simulate a rotation between the emitter and the receiver. The photons then travel through free space for slightly more than a metre to the measurement terminal. At the input of the measurement device, a spectral filter with 10 nm passband and 0.7 maximum transmission is used to reduce background noise. The optical arrangement of the receiver is similar to the emitter except that it is used in reverse. The common optical mode is divided into three beams by the non-PBSs and waveplates are used before the PBSs to allow measurements in the three bases. Thus, the measurement basis is passively selected by the path of the photon, making it perfectly random. The six PBS outputs are combined with approximately 0.8 efficiency to multimode optical fibres leading to single-photon detectors. The photo detectors are silicon avalanche photodiodes with 0.45 efficiency at 850 nm, 400 dark counts per second, a timing resolution of 600 ps and 50 ns deadtime. Their firing times as well as a clock pulse coming from the pattern generator are continuously recorded by a counting card. In post-processing, we eliminate all the counts that happened when another detector was still in its deadtime, i.e. whenever two counts happen within 60 ns. Bitrates could possibly be increased by using...
Figure 3. Results of the normalized detector count matrix for the implemented RFI QKD protocol. Each matrix square represents the number of counts on the specified detector, when the specified polarization was prepared. (a) With the two reference frames aligned, corresponding preparation and measurement bases are almost completely correlated, with measurements between mutually unbiased bases showing almost no correlation. This indicates almost perfect transmission through the quantum channel. (b) Comparison of ideal (I) and measured data (M) for six further reference frames, with angle of misalignment shown. While the counts contributing to the correlator $C_{ZZ}$ remain largely independent of the rotation angle, others contribute a periodic dependence to correlators $C_{XX}$, $C_{XY}$, $C_{YX}$ and $C_{YY}$. Counts contributing to the non-zero correlators $C_{XZ}$, $C_{YZ}$, $C_{ZX}$ and $C_{ZY}$ indicate that the X, Y and Z directions are not perpendicular.

detection events in other detectors during a given detector’s deadtime, but the implications on security are unexplored. The remaining number of counts for a measurement duration of 1 s is approximately $2 \times 10^6$ out of the $250 \times 10^6$ weak pulses generated. The experiment is performed in the dark and owing to spectral filtering background noise is negligible compared to detector dark counts.

Finally, by matching recorded detection times with the original random patterns we can construct a $6 \times 6$ matrix (see figure 3(a)) corresponding to the number of times one of the six detectors fired when one of the six lasers was active. The number of counts is maximal if the emitting and receiving polarizations are the same, it is minimal if they are opposite and it is approximately half of the maximum for all the other polarizations. This matrix constitutes the raw data of the security analysis. The counts in this matrix will be used for two different purposes. Half of the counts when both the sending and the measurement basis were Z are set aside as the raw key. The remaining half with all other counts forms the basis of the parameter estimation. The raw key length for each 1 s interval is approximately $2 \times 10^5$. In order to demonstrate the robustness of our QKD scheme against reference frame rotations, we insert a half waveplate on a rotating mount in the free-space optical path between the two terminals. Varying the optic axis angle of the half waveplate simulates rotations of Alice’s device. For each angle, a measurement is taken similar to that presented in figure 3(a). A comparison between measurement data and the $6 \times 6$ matrix predicted for ideal preparation and detection is shown in figure 3(c). The matching detector count patterns in figure 3(c) already suggest that a quantum channel between the terminals is established, but in order to claim the possibility of QKD we need to analyse the results more rigorously.
3. Secure key fraction

The security of the RFI QKD protocol is discussed in [19]: two parameters are estimated from the measurements: the quantum bit error rate $Q$ and a rotation invariant quantity $C$ (see appendix B). While this analysis gives a good intuition why the scheme is RFI, it does not take into account factors that can impact the keyrate negatively in a real-world setting, such as non-orthogonality of the measurement directions or finite size effects. In this section we derive the secure key fraction in the qubit subspace based on a model of the device including imperfect calibration of preparation and measurement bases, non-uniform detector efficiencies and also the effect of a finite number of measurements. In general, the calculation of the secret key fraction can be posed as an inference problem: given the measurements and a device model what is the maximum amount of information an eavesdropper can possess about the distributed key? We first introduce a simplified expression for the secure key fraction, then consider a model of our QKD system and minimize the secure key fraction subject to constraints derived from the model and the measurements.

The secure key fraction can be reduced from the ideal 100% due to leakage of information at two stages in the protocol [24]. During the quantum stage information can leak to an eavesdropper, while during error correction a certain minimum amount of information needs to be exchanged over a classical channel. The two terms of the following expression [25] for the secret key fraction reflect the impact of those two information leaks

$$r = S(\chi_A|\rho_E) - H(\chi_A|\chi_B),$$

where $S(\cdot|\cdot)$ denotes the conditional von Neumann entropy, $H(\cdot|\cdot)$ the conditional Shannon entropy, $\chi_A$ are the classical bit values at terminal $A$, $\chi_B$ are the classical bit values at terminal $B$ and $\rho_E$ denotes the density matrix of the eavesdropper. The first term describes the entropy of the key bits $\chi_A$ given the eavesdropper’s information, we will call this ‘usable entropy’, $S_U$. The second term is the minimum necessary information to successfully perform error correction at the Shannon limit. In any real-world implementation this number has to be multiplied by a factor larger than one to account for non-ideal error correction schemes. The main objective of the parameter estimation step is to find the minimum usable entropy given the constraints set by the measurements. These constraints also take into account the uncertainties associated with a finite number of performed measurements. Additionally, the parameter estimation step provides information about the bit error rate, which is needed for error correction and thus an estimate for the second term. In our analysis we assume that the measurement results are produced by a two qubit density matrix $\rho_{AB}$ shared between parties $A$ and $B$. The usable entropy can be expressed as (see appendix C)

$$S_U = S(\rho_{AB} \parallel \mathcal{P}_B \rho_{AB}),$$

where $S(A \parallel B)$ denotes the relative entropy and the super-operator $\mathcal{P} \rho = P_0^A \rho P_0^A + P_1^A \rho P_1^A$ with the projector on the bit values at terminal $A$ defined as $P^A_{0/1} = \frac{1}{2}(1 \pm \sigma_A^z)$. To estimate the usable entropy we have to establish a model for our QKD system. This consists of a model of the quantum channel, embodied in the density matrix, along with a model of the terminal devices. The secret key fraction can be obtained as the minimum over all channel and device parameters that are consistent with the performed measurements. For a finite number of measurements, the constraints will possess a statistical uncertainty that has to be taken into account in the minimization procedure. As we are looking for an upper bound for the usable entropy, it suffices
to consider a simplified density matrix (see appendix D), guaranteed to give a lower usable entropy than the full density matrix. The usable entropy for this density matrix becomes

$$S_U(\lambda_1, \lambda_2) = 1 + \sum_i \eta_i \log_2 \eta_i - h(2\eta_1)$$

(3)

with the eigenvalues of the density matrix $\eta_1 = \eta_2 = 1/4(1 - \lambda_1)$, $\eta_3 = 1/4(1 + \lambda_1 - 2\lambda_2)$ and $\eta_4 = 1/4(1 + \lambda_1 + 2\lambda_2)$ and $h(x) = -x \log_2 x - (1-x) \log_2(1-x)$. With perfectly calibrated and aligned devices no additional model parameters have to be taken into account. Imperfect measurement devices can lead to a large number of additional parameters, such as non-orthogonalities in the preparation and measurement bases and detector efficiencies, which can be collected into the vector $\alpha$ (for the details of the model see appendix E). The usable entropy is obtained as the minimum over all parameters $\alpha, \lambda_1/2$

$$S_{\text{min}} = \min_{\alpha, \lambda_1, \lambda_2} S_U(\lambda_1, \lambda_2).$$

(4)

The parameters have to obey the constraints imposed by the observations

$$f_i(m) - \sigma \delta f_i(m) \leq f_i[q(\alpha, \lambda_1, \lambda_2)] \leq f_i(m) + \sigma \delta f_i(m),$$

(5)

where $m$ is a matrix containing all relevant detector counts, $q$ is the corresponding probability of observing a detector count according to the device model (see appendix E), the $f_i$ are the functions defining the different constraints, the $\delta f_i$ are their corresponding variances and $\sigma$ is chosen to give a certain probability that the estimated usable entropy is too high. In our parameter estimation step we use a set of 21 constraints (see appendix F) consisting of nine correlation functions $C_{AB}$, $A, B = X, Y, Z$, the six probabilities that a photon was prepared in a certain polarization direction $P_{A\pm}$, $A = X, Y, Z$ and the six probabilities to detect in a certain detector $D_{B\pm}$, $B = X, Y, Z$. For each function $f_i$ we can give the standard deviation $\delta f_i$ (see appendix F). To obtain the secret key fraction, we need to subtract the observed relative entropy in the key basis from the usable entropy

$$r = S_{\text{min}} - h\left(\frac{1 - C_{ZZ} + \sigma \delta C_{ZZ}}{2}\right).$$

(6)

The full set of measurements enables us to calculate an RFI keyrate. From the detector counts we can construct nine correlation functions

$$C_{AB} = \frac{m_{++}^{AB} + m_{+-}^{AB} - m_{+}^{AB} - m_{++}^{AB}}{m_{++}^{AB} + m_{+-}^{AB} + m_{+}^{AB} + m_{++}^{AB}}, \quad A, B = X, Y, Z,$$

(7)

where the $m_{++}^{AB}$ are the four different detector counts given that the qubit was prepared in direction $A\pm$ and detected in direction $B\pm$. In the case of orthonormal preparation and measurement bases these can be directly identified with the qubit correlation functions. A secret key fraction can be obtained as the minimum keyrate over all density matrices consistent with the observed correlators. In the BB84 protocol [25, 26] only two correlators, e.g. $C_{XX}$ and $C_{ZZ}$, are used as constraints. When the reference frames are rotated $C_{XX}$ will drop and so will the secret key fraction. The RFI QKD scheme uses the four correlators $C_{XX}$, $C_{XY}$, $C_{YX}$, $C_{YY}$ as well as $C_{ZZ}$. While each individual correlator may decrease under reference frame rotations, the combination $C = C_{XX}^2 + C_{XY}^2 + C_{YX}^2 + C_{YY}^2$ ideally stays constant, enabling RFI secret key fractions. In order to treat imperfect preparation and measurement, we have to depart from the assumption of orthonormal bases and include a more detailed detector model. Each preparation and each detector are associated with a direction on the Poincaré sphere, given by a
unit vector. Since we aim to use the $z$-basis for the key bits we can identify two preparation
directions with the $\pm z$ direction on the Poincaré sphere, without overestimating the secret
key fraction. Each direction is parametrized by two variables (e.g. azimuth and polar angles),
resulting in a total of 20 free parameters (see appendix E). Different absorptions may occur
in the preparation channels, and similarly detectors may have different efficiencies. With six
possible preparation directions and six possible detection directions this adds another set of 12
parameters. The quantum channel can be represented by a two-parameter two-qubit density
matrix in a simplification over the more commonly employed Bell diagonal density matrix
(see appendix D). This results in a model with 34 free parameters. The secret key fraction is
then obtained as the minimum over all parameters that fulfil the constraints imposed by the
measurements, e.g. from the correlators $C_{AB}$; in our case a set of 21 constraints. For the number
of detector counts approaching infinity the constraints are equalities, but for a finite number of
observations the value can lie within an interval determined by the number of counts and the
desired uncertainty. A small number of counts will lead to larger uncertainty in the correlation
function and therefore to lower results for the secret key fraction.

4. Results and discussion

Our main result is that the secret key fraction remains above 0.2 for all rotation angles even in
the presence of device imperfections, see U-RFI in figure 4. To better understand the calculated
keyrate we make a comparison with established protocols: the BB84 protocol and the RFI
QKD protocol as proposed by Laing et al [19]. For the sake of comparison we assume that
in these protocols both preparation bases and measurement bases are perfect, i.e. the measured
correlation functions are indeed the qubit correlation functions of the underlying density matrix.
A summary of the calculation of the BB84 and RFI QKD keyrates can be found in appendices A
and B. We clearly see in figure 4 that while the BB84 keyrate drops to zero for certain angles the
RFI QKD keyrate remains non-zero for all rotation angles. The plot also shows that for certain
angles the RFI secret key fraction estimate is too optimistic compared to the U-RFI rates. This
happens due to non-orthogonal measurement directions, which are not taken into account in
the RFI QKD security analysis. The distinct peaks in the secret key fraction coincide with the
peaks visible in the secret key fraction calculated for the BB84 protocols, as outlined above.
This can be understood in the following way: the secret key fraction we calculate depends on
the correlators $C_{AB}$, $A, B = X, Y, Z$. The correlator $C_{ZZ}$ is linked to the qubit error rate. The
correlators $C_{XX}, C_{XY}, C_{YX}, C_{YY}$ are related to monitoring the eavesdropping. If the absolute
value of one of these correlators is large then eavesdropping in the key basis is small, even if
other correlators are relatively small. This also makes the secret key fraction larger than the RFI
keyrate for some angles. In the region between the peaks no individual correlator is large and
only their combination gives a positive secret key fraction. In the presence of alignment errors
some of the contributing correlators may be small and as a result the secret key fraction drops.

During each transmission of 1 s we set aside approximately $2 \times 10^5$ raw key bits. After
obtaining the correct secret key fraction from the parameter estimation step, we can perform
the privacy amplification step by applying the appropriate two-universal hash function (e.g. a
Toeplitz matrix [27]) to the raw key and obtain a secure key. With a secret key fraction of
around 0.25 we arrive at an approximate keyrate of $5 \times 10^4 s^{-1}$. In the current implementation
of our scheme potential security loop holes exist due to side channels [28], the most obvious one
coming from the use of six different lasers in the preparation stage. While this loophole can be
Figure 4. Keyrates as a function of the physical waveplate rotation angle for two RFI and four different BB84 protocols. U-RFI labels the RFI keyrate assuming uncalibrated devices. It is obtained from numerical minimization over the full set of model parameters subject to constraints imposed by the measurements. The blue dots correspond to the minimized keyrate neglecting the variance coming from the finite number of measurements. The blue bars indicate the result obtained by allowing for an uncertainty in the estimate of the constraints of three times the standard deviation. The remaining curves are obtained from the same data but with a simplified model, assuming orthogonality within bases and total perpendicularity between bases. RFI labels the keyrate for the RFI protocol as outlined in [19]. XX, XY, YX and YY label the keyrates for the BB84 protocol using the respective correlator pairs $C_{ZZ}$ and $C_{XX}$, $C_{ZZ}$ and $C_{XY}$, and so on.

plugged by using a single laser and a $1 \times 6$ optical switch further analysis of the impact of side channels on the keyrate is required (e.g. the effect of photon number statistics [29] or detector characteristics [30] on our scheme).

Nevertheless, we are able to give an estimate of the impact of photon number statistics on the keyrate in our scheme. Without employing decoy states we have to assume that in pulses that contain more than one photon and which are contributing to the raw key all information is lost to the eavesdropper. Our photon source generates weak coherent pulses with a rate of 250 MHz and an average photon number of 0.05 per pulse. In order to assess the impact of a hypothetical photon number splitting attack, we have to characterize the quantum channel. An important quantity is the accessible loss [31] in the quantum channel, i.e. the part of the loss that is, in principle, under the control of the eavesdropper. Due to the short-range free-space transmission, no absorption occurs between Alice and Bob. A small amount of absorption (coupling efficiency $\approx 0.8$) can be attributed to the mode mismatch between sender and receiver and could be manipulated by an eavesdropper. All other losses occur in the Bob device and are inaccessible losses. Starting from a 250 MHz pulse rate and 0.05 photons per pulse we arrive at
a raw single-photon rate of 12.5 MHz. The recorded photon count rate is 2 MHz, giving a total absorption of $\eta = 0.16$. The accessible part of the absorption is $\eta_A = 0.8$, while the inaccessible part, containing absorption in filters, losses in optical components and finite detector efficiency contributes $\eta_I = 0.2$, so that $\eta = \eta_A \eta_I$. The rate of two-photon pulses according to Poisson statistics is 0.3 MHz. The remaining single photons after a photon number splitting attack will still experience the inaccessible losses, so that the total number of recorded detector clicks associated with two-photon pulses is 60 kHz. Of these photons only a fraction contributes to the raw key. For our setup that fraction is 0.1. For a key distribution lasting 1 s we estimate that an eavesdropper can at most have information about 6000 key bits out of $2 \times 10^5$ key bits, or the secure key fraction has to be reduced by approximately 0.03, due to the probabilistic nature of the photon source, only slightly modifying our secret key fraction.

In summary, we have shown the feasibility of RFI key distribution using off the shelf bulk optical components in a compact assembly. Our setup uses passive components and can readily be transferred to a miniaturized version using integrated optics on a chip [32, 33]. Our analysis employed in the parameter estimation step obviates the need for precise alignment of the preparation and measurement qubit bases. The achievable keyrates are sufficient to distribute hundreds of 256 bit keys within 1 s. In order to realize a handheld QKD device additional functionality, like steering of the emitted photons, towards a receiver needs to be implemented. Possible solutions include movable mirrors, movable lenses or phased arrays. Overall, the work presented here paves the way for mass-produced handheld QKD devices.

### Appendix A. Keyrate for BB84

For the calculation of the keyrate for the BB84 protocol we follow [25], with the difference that we use two parameters for the quantum channel, the correlation functions $C_{XX}$ and $C_{ZZ}$. The secure key fraction for the BB84 protocol is given by

$$r = \min_{\eta_i} \left( 1 + \sum_{i=1}^{4} \eta_i \log_2 \eta_i \right)$$  \hspace{1cm} (A.1)

under the constraints

$$C_{XX} = 1 - 2 \eta_2 - 2 \eta_4,$$  \hspace{1cm} (A.2)

$$C_{ZZ} = 1 - 2 \eta_3 - 2 \eta_4,$$  \hspace{1cm} (A.3)

$$\sum_{i=1}^{4} \eta_i = 1.$$  \hspace{1cm} (A.4)

This can be solved analytically to give

$$r = 1 + z_+ x_+ \log_2(z_+ x_+) + z_+ x_- \log_2(z_+ x_-) + z_- x_+ \log_2(z_- x_+) + z_- x_- \log_2(z_- x_-)$$  \hspace{1cm} (A.5)

with

$$x_\pm = \frac{1 \pm C_{XX}}{2}, \quad z_\pm = \frac{1 \pm C_{ZZ}}{2}.$$  \hspace{1cm} (A.6)

Alternatively other correlators than $C_{XX}$ can be used to obtain a keyrate. In the case of misaligned reference frames the correlators $C_{XY}$ or $C_{YX}$ may give a more favourable keyrate.
Appendix B. Reference frame independent quantum key distribution

RFI QKD was introduced in [19]. The scheme solves the problem of aligning reference frames between two partners in a QKD protocol if one stable direction exists (e.g. in polarization encoding physical rotation does not influence the circular polarization direction). The stable direction is used for encoding the qubits, while perpendicular directions are used for parameter estimation. It is sufficient to consider two quantities constructed from the qubit correlation functions: the bit error rate

\[ Q = \frac{1 - C_{ZZ}}{2} \]  

(B.1)

and the quantity

\[ C = C_{XX}^2 + C_{XY}^2 + C_{YX}^2 + C_{YY}^2 \]  

(B.2)

with the qubit correlation functions given by

\[ C_{AB} = \text{Tr} (\sigma_A \sigma_B \rho), \]  

(B.3)

where \( \rho \) is the two qubit density matrix. Under rotations around the z-axis the Pauli matrices transform \( \sigma_x \rightarrow \sigma_x \cos \alpha + \sigma_y \sin \alpha \) and \( \sigma_y \rightarrow \sigma_y \cos \alpha - \sigma_x \sin \alpha \), with the rotation angle given by \( \alpha \). One can see that the quantity \( C \) stays invariant under these kinds of rotations. The secret key fraction can be shown to be a function of \( C \) and \( Q \). For \( Q \ll 0.159 \) the secret key fraction becomes

\[ r = 1 - h(Q) - (1 - Q)h \left( \frac{1 + u}{2} \right) - Qh \left( \frac{1 + v}{2} \right) \]  

(B.4)

with \( h(x) = -\log_2 x - (1 - x) \log_2 (1 - x) \) the Shannon entropy function and \( u = \min(\sqrt{C/2}/(1 - Q), 1) \) and \( v = \sqrt{C/2 - (1 - Q)^2 u^2}/Q \).

Appendix C. Conditional entropy decreases under projective measurement

A quantum communication channel between parties Alice (A) and Bob (B) can be described by the density matrix \( \rho_{AB} \). In general, this density matrix will not be pure due to noise, errors and the action of an eavesdropper. In order to prove security of the communication channel, we have to assume all deviations from the ideal case are due to an eavesdropper. The combined state of \( \rho_{AB} \) and an eavesdropper can then be expressed as the pure state

\[ |\psi\rangle_{ABE} = \sum_{i=1}^{4} \sqrt{\lambda_i} |\Phi_i\rangle_{AB} |v_i\rangle_E, \]  

(C.1)

where the \( \lambda_i \) are the eigenvalues of \( \rho_{AB} \), \( |\Phi_i\rangle_{AB} \) are the corresponding eigenfunctions and \( |v_i\rangle \) are an orthogonal basis for the state of the eavesdropper. Note that the dimension of the Hilbert space of the eavesdropper equals the dimensions of \( \rho_{AB} \). The density matrices in the subspaces can then be obtained as

\[ \rho_{AB} = \text{Tr}_E (|\psi\rangle_{AB} \langle \psi|_{AB}) \]  

(C.2)

and

\[ \rho_E = \text{Tr}_{AB} (|\psi\rangle_{AB} \langle \psi|_{AB}). \]  

(C.3)
The reduced density matrix of the eavesdropper equals the reduced density matrix of Alice and Bob up to a unitary transformation
\[ \rho_E = U \rho_{AB} U^\dagger. \]  
(C.4)

Let us consider the entropy of the key bits \( \chi_A \) given that the eavesdropper knows the state of the system \( \chi_E \), \( S(\chi_A|\chi_E) \). We can rewrite the conditional entropy as
\[ S(\chi_A|\rho_E) = S(\chi_A) + S(\chi_E|\chi_A) - S(\rho_E). \]  
(C.5)

With \( X \) being the classical value of Alice’s qubit we can write
\[ S(\rho_E|\chi_A) = \sum_{x=0,1} p_x S(E_x). \]  
(C.6)

If Alice prepares key bit 0 with probability \( p_0 \) and key bit one with probability \( p_1 \) we can write the corresponding density matrices \( E_0, E_1 \) with the help of the projection operators
\[ E_x = \text{Tr}_{AB} (P_x |\psi\rangle_{AB} \langle \psi|_{AB}) \]  
(C.7)

or
\[ E_x = \frac{1}{p_x} \sqrt{\rho_{AB}} P_x \sqrt{\rho_{AB}}. \]  
(C.8)

Since unitary transformations do not change the entropy we can replace \( \rho_{AB} \) with \( \rho_E \) in the calculation of entropies
\[ S\left( \frac{1}{p_x} \sqrt{\rho_{AB}} P_x \sqrt{\rho_{AB}} \right) = S\left( \frac{1}{p_x} \sqrt{\rho_E} P_x \sqrt{\rho_E} \right). \]  
(C.10)

We can use
\[ \text{Tr}[\sqrt{\rho P} \sqrt{\rho} F(\sqrt{\rho P} \sqrt{\rho})] = \text{Tr}[P \rho F(\rho P)], \]  
(C.11)

where \( F \) is any function and we used
\[ F(\sqrt{\rho P} \sqrt{\rho}) = \sum_n c_n (\sqrt{\rho P} \sqrt{\rho})^n = \sum_n c_n \sqrt{\rho P} (\rho P)^{n-1} P \sqrt{\rho}. \]  
(C.12)

We can therefore write
\[ S(\rho_E|\chi_A) = \sum_{x=0,1} p_x S\left( \frac{1}{p_x} P_x \rho_E P_x \right). \]  
(C.13)

Since the \( P_x \) project onto orthogonal subspaces we can use (see [34, p 518]) to write
\[ S(\rho_E|\chi_A) = S \left( \sum_{x=0,1} P_x \rho_E P_x \right) - S(\chi_A). \]  
(C.14)

The equality holds if the projectors \( P_x \) project onto orthogonal subspaces and acts as an upper bound on the usable entropy otherwise. The conditional entropy therefore becomes
\[ S(\chi_A|\rho_E) = S \left( \sum_{x=0,1} P_x \rho_E P_x \right) - S(\chi_E). \]  
(C.15)
Introducing the projective measurement
\[ \mathcal{P} \rho = \sum_x P_x \rho P_x \]  
we can write
\[ S(\chi_A|\rho_E) = S(\mathcal{P} \rho_E) - S(\rho_E). \]  
(C.17)

Since \( \mathcal{P} \) is a projective measurement this simplifies further to the relative entropy
\[ S(\chi_A|\rho_E) = S(\rho_E \parallel \mathcal{P} \rho_E) = S(\rho_{AB} \parallel \mathcal{P} \rho_{AB}). \]  
(C.18)

We now want to investigate how a further projective measurement influences the relative entropy. Introducing
\[ \mathcal{L} \rho = \sum_i L_i \rho L_i \]  
(C.19)

with the projection operators \( L_i \). We consider the relative entropy before and after the projective measurement \( \mathcal{L} \)
\[ S(\rho_{AB} \parallel \mathcal{P} \rho_{AB}) - S(\mathcal{L} \rho_{AB} \parallel \mathcal{P} \mathcal{L} \rho_{AB}). \]  
(C.20)

For commuting operations
\[ \mathcal{P} \mathcal{L} = \mathcal{L} \mathcal{P} \]  
(C.21)

and using that the relative entropy of two density matrices decreases or stays the same under completely positive trace preserving maps [35] we obtain
\[ S(\rho_{AB} \parallel \mathcal{P} \rho_{AB}) - S(\mathcal{L} \rho_{AB} \parallel \mathcal{L} \mathcal{P} \rho_{AB}) \geq 0 \]  
(C.22) 

if the operations \( \mathcal{L} \) and \( \mathcal{P} \) commute.

Appendix D. Simplified density matrices for parameter estimation

We can use the inequality above to simplify the model density matrix for parameter estimation. Starting from the full two qubit density matrix with 15 free parameters we can apply a series of projective measurements
\[ \mathcal{L} = \mathcal{L}_2 \mathcal{L}_1 \]  
(D.1)

to arrive at a simpler density matrix with fewer parameters that is guaranteed to give a smaller value for the usable entropy. The individual projective measurement super-operators are
\[ \mathcal{L}_i = \lim_{t \to \infty} e^{-t \mathcal{K}_i} \]  
(D.2)

and the corresponding Liouvillian
\[ \mathcal{K}_i \rho = \{ \Sigma_i, \Sigma_i, \rho \} - 2 \Sigma_i \rho \Sigma_i, \quad \Sigma_1 = \sigma_z^A - \sigma_z^B, \quad \Sigma_2 = \sigma_x^A \sigma_x^B. \]  
(D.3)

If we use the \( z \) basis for the key bits then the measurement operator becomes
\[ \mathcal{P} \rho = P^A_0 \rho P^A_0 + P^A_1 \rho P^A_1 \]  
(D.4)

with the projector on the bit values at terminal \( A \) defined as
\[ P^A_{0/1} = \frac{1}{2} \left( 1 \pm \sigma_z^A \right). \]  
(D.5)

New Journal of Physics 15 (2013) 073001 (http://www.njp.org/)
It can be shown that
\[
\mathcal{P}\mathcal{L}_i \rho - \mathcal{L}_i \mathcal{P} \rho = 0
\] (D.6)
for all density matrices \( \rho \). After applying all the projective measurements to a general density matrix the simplified density matrix takes the form
\[
\rho = \frac{1}{4} \begin{pmatrix}
1 + \lambda_1 & 0 & 0 & 2\lambda_2 \\
0 & 1 - \lambda_1 & 0 & 0 \\
0 & 0 & 1 - \lambda_1 & 0 \\
2\lambda_2 & 0 & 0 & 1 + \lambda_1
\end{pmatrix}
\] (D.7)
This density matrix can now be used in models for parameter estimation.

**Appendix E. Device model**

We want to construct a model for the probability of registering a detector count in the detector measuring in basis \( B \), direction \( V \), provided the bit was prepared in basis \( A \), direction \( U \), \( p_{AB}^{UV} \).

The probability of observing a count in a detector given a certain preparation is proportional to
\[
q_{AB}^{UV} = t_1^A U t_2^B V \text{Tr}(\hat{P}_A U \hat{P}_B V \rho),
\] (E.1)
where \( t_1 \) and \( t_2 \) account for the preparation and detection efficiencies. The projectors \( \hat{P}_A U \) and \( \hat{P}_B V \) are along a certain preparation or measurement direction, given by a unit vector \( n_{AX} \) or \( r_{BY} \)
\[
\hat{P}_A U = \frac{1}{2} (1 + n_{AX} \cdot \sigma_A), \quad \hat{P}_B V = \frac{1}{2} (1 + r_{BY} \cdot \sigma_B),
\] (E.2)
where \( \sigma_A/B \) is a vector of Pauli matrices in the respective local basis. Using the simplified density matrix equation (D.7), we obtain
\[
q_{AB}^{UV} = \frac{t_1^A U t_2^B V}{4} \left[ 1 + \sum_{ij} n_i^A U r_j^B V \text{Tr}(\hat{\sigma}_i^A \hat{\sigma}_j^B \rho) \right]
\] (E.3)
with
\[
\text{Tr}(\hat{\sigma}_i^A \hat{\sigma}_j^B \rho) = \delta_{ij} I = \Lambda_{ij}, \quad I = (\lambda_2, \lambda_2, \lambda_1)
\] (E.4)
and therefore
\[
q_{AB}^{UV} = \frac{t_1^A U t_2^B V}{4} (1 + n_{AX} \cdot \Lambda \cdot r_{BY}),
\] (E.5)
so that the probabilities become
\[
P_{AB}^{UV} = \frac{q_{AB}^{UV}}{\sum_{ABUV} q_{AB}^{UV}}.
\] (E.6)
For our measurement setup there are six distinct preparation directions \( n_{AU} \), \( A = X, Y, Z \), \( U = \pm \), with two free parameters, the azimuthal and polar angles, specifying each direction. The \( z \)-direction is identified with the qubit directions at terminal A and therefore we fix \( n_{Z \pm} = (0, 0, \pm 1) \). Similarly there are six measurement directions \( r_{BV} \), \( B = X, Y, Z \), \( V = \pm \).
Appendix F. Detector counts and correlation functions

The calculation of the secret key fraction is based on a minimization subject to a number of constraints. In our implementation we use a total of 21 constraints. Each constraint and its corresponding standard deviation can be calculated from the raw detector counts obtained in the parameter estimation process. The first set of constraints is given by the nine correlation functions

\[ C_{AB}(m) = \frac{m_{++}^A + m_{--}^A - m_{+-}^A - m_{-+}^A}{m_{++}^B + m_{--}^B + m_{+-}^B + m_{-+}^B}, \quad A, B = X, Y, Z. \] (F.1)

Additional six constraints are the probabilities for preparing a certain direction

\[ P_{AU}(m) = \frac{\sum_{BV} m_{UV}^A}{N_0}, \quad N_0 = \sum_{ABUV} m_{UV}^A, \] (F.2)

where \( N_0 \) is the total number of detector counts. Further six constraints are the probabilities for detecting a certain direction

\[ D_{BV}(m) = \frac{\sum_{AU} m_{UV}^A}{N_0}. \] (F.3)

The corresponding standard deviations are

\[ \delta C_{AB}(m) = \sqrt{\frac{4 \left( m_{++}^A + m_{--}^A \right) \left( m_{+-}^A + m_{-+}^A \right)}{\left( m_{++}^B + m_{--}^B + m_{+-}^B + m_{-+}^B \right)^3}}, \] (F.4)

and

\[ \delta P_{AU}(m) = \sqrt{\frac{(N_0 - \sum_{BV} m_{UV}^A) \sum_{BV} m_{UV}^A}{N_0^3}}, \] (F.5)

as well as

\[ \delta D_{BV}(m) = \sqrt{\frac{(N_0 - \sum_{AU} m_{UV}^A) \sum_{AU} m_{UV}^A}{N_0^3}}. \] (F.6)

This gives us a total of 21 constraints derived from the raw detector counts to be used in the calculation of the secret key fraction.

References

[1] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 Quantum cryptography Rev. Mod. Phys. 74 145–95
[2] Bennett C H and Brassard G 1984 Int. Conf. on Computers, Systems and Signal Processing (Bangalore) pp 175–9
[3] Ekert A K 1991 Quantum cryptography based on Bell’s theorem Phys. Rev. Lett. 67 661–3
[4] Stucki D et al 2011 Long-term performance of the SwissQuantum quantum key distribution network in a field environment New J. Phys. 13 123001

New Journal of Physics 15 (2013) 073001 (http://www.njp.org/)

\[ \text{New Journal of Physics 15 (2013) 073001 (http://www.njp.org/)} \]
Sasaki M et al 2011 Field test of quantum key distribution in the Tokyo QKD network Opt. Express 19 10387
Peev M et al 2009 The SECOQC quantum key distribution network in Vienna New J. Phys. 11 075001
Dixon A R, Yuan Z L, Dynes J F, Sharpe A W and Shields A J 2010 Continuous operation of high bit rate quantum key distribution Appl. Phys. Lett. 96 161102
Dynes J F et al 2009 Efficient entanglement distribution over 200 kilometers Opt. Express 17 11440
Mirza A and Petruccione F 2011 Recent findings from the quantum network in Durban AIP Conf. Proc. 1363 35–8
Hughes R J, Nordholt J E, Derkacs D and Peterson C G 2002 Practical free-space quantum key distribution over 10 km in daylight and at night New J. Phys. 4 43
Alléaume R, Treussart F, Messin G, Dumeige Y, Roch J-F, Beveratos A, Brouri-Tualle R, Poizat J-P and Grangier P 2004 Experimental open-air quantum key distribution with a single-photon source New J. Phys. 6 92
Ursin R et al 2007 Entanglement-based quantum communication over 144 km Nature Phys. 3 481–6
Schmitt-Manderbach T et al 2007 Experimental demonstration of free-space decoy-state quantum key distribution over 144 km Phys. Rev. Lett. 98 010504
Godfrey M S, Lynch A M, Duligall J L, Munro W J, Harrison K J and Rarity J G 2006 Free-space secure key exchange from 1 m to 1000 km Proc. SPIE 6399 63990E
Duligall J L, Godfrey M S, Harrison K A, Munro W J and Rarity J G 2006 Low cost and compact quantum key distribution New J. Phys. 8 249
Boileau J-C, Laflamme R, Laforest M and Myers C R 2004 Robust quantum communication using a polarization-entangled photon pair Phys. Rev. Lett. 93 220501
Chen T-Y, Zhang J, Boileau J-C, Jin X-M, Yang B, Zhang Q, Yang T, Laflamme R and Pan J-W 2006 Experimental quantum communication without a shared reference frame Phys. Rev. Lett. 96 150504
D’Ambrosio V, Nagali E, Walborn S P, Aolita L, Slussarenko S, Marrucci L and Sciarrino F 2012 Complete experimental toolbox for alignment-free quantum communication Nature Commun. 3 961
Laing A, Scarani V, Rarity J G and O’Brien J L 2010 Reference-frame-independent quantum key distribution Phys. Rev. A 82 012304
Acín A, Brunner N, Gisin N, Massar S, Pironio S and Scarani V 2007 Device-independent security of quantum cryptography against collective attacks Phys. Rev. Lett. 98 230501
Sheridan L, Phuc Le T and Scarani V 2010 Finite-key security against coherent attacks in quantum key distribution New J. Phys. 12 123019
Meyer T, Kampermann H, Kleinmann M and Bruß D 2006 Finite key analysis for symmetric attacks in quantum key distribution Phys. Rev. A 74 042340
Scarani V and Renner R 2008 Quantum cryptography with finite resources: unconditional security bound for discrete-variable protocols with one-way postprocessing Phys. Rev. Lett. 100 200501
Scarani V, Bechmann-Pasquinucci H, Cerf N J, DuMerk , Lütkenhaus N and Peev M 2009 The security of practical quantum key distribution Rev. Mod. Phys. 81 1301–50
Renner R, Gisin N and Kraus B 2005 Information-theoretic security proof for quantum-key-distribution protocols Phys. Rev. A 72 012332
Bennett C H, Brassard G and Mermin N D 1992 Quantum cryptography without Bell’s theorem Phys. Rev. Lett. 68 557–9
Krawczyk H 1995 New Hash Functions for Message Authentication (Lecture Notes in Computer Science vol 921) pp 301–10
Nauerth S, Fürst M, Schmitt-Manderbach T, Weier H and Weinfurter H 2009 Information leakage via side channels in freespace BB84 quantum cryptography New J. Phys. 11 065001
Lo H-K, Ma X and Chen K 2005 Decoy state quantum key distribution Phys. Rev. Lett. 94 230504
Jain N, Wittmann C, Lydersen L, Wiechers C, Elser D, Marquardt C, Makarov V and Leuchs G 2011 Device calibration impacts security of quantum key distribution Phys. Rev. Lett. 107 110501
Lütkenhaus N and Jahma M 2002 Quantum key distribution with realistic states: photon-number statistics in the photon-number splitting attack New J. Phys. 4 44

New Journal of Physics 15 (2013) 073001 (http://www.njp.org/)
[32] Politi A, Cryan M J, Rarity J G, Yu S and O’Brien J L 2008 Silica-on-silicon waveguide quantum circuits Science 320 646–9
[33] O’Brien J L, Furusawa A and Vučković 2009 Photonic quantum technologies Nature Photon. 3 687–95
[34] Nielsen M A and Chuang I L 2010 Quantum Computation and Quantum Information 1st edn (Cambridge Series on Information and the Natural Sciences) (Cambridge: Cambridge University Press)
[35] Lindblad G 1975 Completely positive maps and entropy inequalities Commun. Math. Phys. 40 147–51