

Characterising a handheld quantum key distribution system with emulated beam steering

David Lowndes^a, Andy Schreier^b, Dominic O’Brien^b, and John Rarity^a

^aDepartment of Electrical and Electronic Engineering, University of Bristol, Woodland Road, Bristol, BS8 1UB, UK

^bDepartment of Engineering Science, University of Oxford, Parks Road, Oxford, OX1 3PJ, UK

ABSTRACT

We present a miniaturised free-space quantum key distribution (QKD) system which allows key exchange between a handheld transmitter and a fixed terminal. The QKD system requires to be optically aligned emphasising the need of a beamsteering unit for later applications. To maintain within the size, weight and power restrictions, the active beamsteering hardware is exclusively located inside the receiver. Our target is consumer use so we present rigorous characterisation against a range of background light levels to show anticipated performance outside of a laboratory environment.

Experimental results show a reduction in the raw count rate commensurate with the transmission of the added components (74.5%) and a small degradation of the error rate (0.5 percentage points) due to the worse signal-to-noise ratio. These combine to a 50% reduction in estimated secret key rate of the system with the additional components for beam steering.

Keywords: QKD, quantum communications, beamsteering, optics, quantum key distribution, security

1. INTRODUCTION

Data security is an ever-increasing concern, and quantum key distribution (QKD) has the potential to form part of future secure infrastructure. Backbone links can be provided by fibre optic^{1–4} or high specification free space links (to satellites, for example^{5–9}). In this paper we discuss a QKD system which could widen access to a QKD backbone network and allow ad-hoc access to untrained users.

A miniaturised free-space QKD system which allows key exchange between a handheld transmitter and a fixed terminal is currently under development. The transmitter has the size of a credit card, weighs 65g, consumes 3.15W of power and consists of widely available components.¹⁰ These transmitter specifications allow for mass-produced low-cost consumer devices in the form of a handheld device. However, the QKD system requires to be optically aligned emphasising the need of a beamsteering unit for any kind of widespread deployment to untrained users. To attain the size, weight and power restrictions of the transmitter, the active beamsteering hardware is exclusively located inside the receiver.

The beamsteering requires real time tracking accuracy sufficient to allow the collimated QKD beam to be coupled into the receiver whilst providing a wide field of view allowing the handheld transmitter to move relatively freely. Our solution is a multistage beamsteering unit using an optical beacon launched from the handheld as a tracking signal. This is a significant modification to both transmitter and receiver and in this paper we quantify the impact to the system by inserting representative components into the optical path of our existing QKD system.

Further author information: (Send correspondence to DL)

DL: E-mail: david.lowndes@bristol.ac.uk

AS: E-mail: andy.schreier@eng.ox.ac.uk

2. EMULATED BEAMSTEERING

Mirror-based beamsteering approaches are wavelength transparent¹¹ and can minimise steering losses allowing for maximum transmission rates.^{12,13} A QKD handheld showing dynamic motion compensation was demonstrated with symmetrical steering mirrors.¹⁴ However, there is a trade-off between large angle coverage and steering refresh rates within a given steering accuracy. A multistage beamsteering system avoids this trade-off by splitting the tasks allowing for real-time steering updates over a wide field of view. This approach comes at the costs of introducing a beam splitter in the quantum channel and therefore affecting the secret key rate.

The beamsteering system uses a beacon signal colinear with the quantum signal using a different wavelength. The beacon and quantum signals are separated inside the receiver terminal and directed onto their respective detectors. Since the tracking is multistage, dichroic elements are not suitable for all of the splitting operations needed inside the QKD receiver. Dichroic elements are also not sufficient to block the beacon from entering the quantum channel so additional filtering is also required.

Fig. 1 shows how the QKD system from,¹⁰ modified by adding a 33:67 beamsplitter (Thorlabs CM1-BP133) and an additional bandpass filter (Thorlabs FBH650-10). This splitting ratio corresponds to the fraction of the channel required for each beamsteering stage, and a filter of sufficient width to pass all of the quantum signal (650nm) but block the beacon (517nm) to fully isolate the QKD receiver optics from the tracking beacon signal.

Aside from the expected additional losses incurred by the addition of the extra components, we quantify the general QKD performance of the system which will also include any effects due to the polarization and signal-to-noise ratio performance of the components.

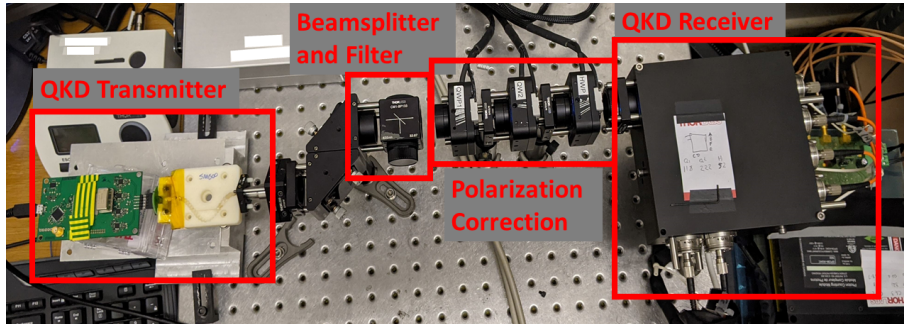


Figure 1. The apparatus used in this work. The QKD transmitter, polarization correction, and QKD receiver are unchanged from,¹⁰ the additional components added are shown in the figure labelled as “beamsplitter and filter”. The beamsplitter is easily removable from the system by unmounting its cage cube from the rest of the system.

3. RESULTS

A variable brightness lamp used to simulate ambient light whilst the QKD system repeatedly operated, collecting 5 million time tags per collection. The lamp was set to gradually decrease brightness until off over half an hour. This produces a varying background from a well lit indoor room, to ideal dark lab conditions.

Figure 2 shows that over the range of background counts, the extracted signal counts remain largely the same. This behaviour is due to fact that the noise is randomly distributed in time. The presence of the beamsplitter can be clearly seen as it causes a reduction in the average signal rate of 74.5%. The datasheet value of the transmission of the CM1-BP133 beamsplitter at 650nm is 78.6%.

The error rate is slightly increased with the beamsplitter inserted, with the average 0.5 percentage points higher. This is likely due to the decreased signal-to-noise ratio and is well within acceptable bounds given the range of error rates across the experiment are up to 2 percentage points.

The calculated secret key rates (using¹⁵) in Fig. 3 are low, due to the low inherent mean photon number of the transmitter. The trends are still valuable as in our comparison the transmitter mean photon number is constant across experiments. The two trends shown in figure 2 of slightly increased error rate and slightly decreased signal rate combine to contribute a 50% reduction in estimated secret key rate for the emulated beamsteering system.

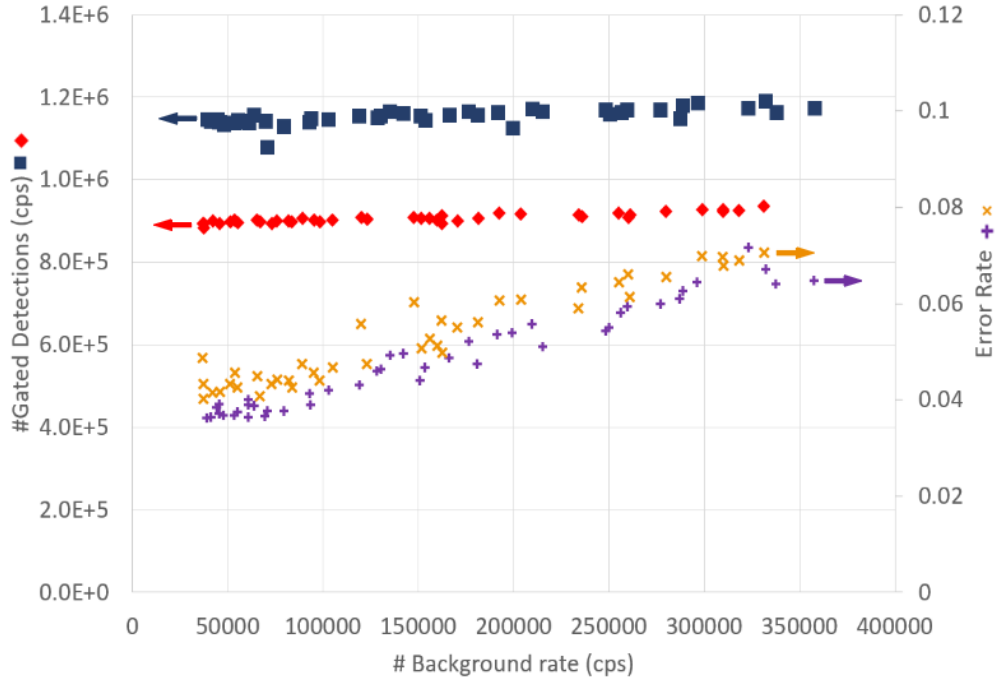


Figure 2. The raw key rate, and error rate for a range of background count rates. Background count rate is estimated by using the number of counts falling outside of the gate width. The blue squares and purple pluses are for the QKD system without the beamsplitter, the red diamonds and orange crosses are for the QKD system with the beamsplitter inserted.

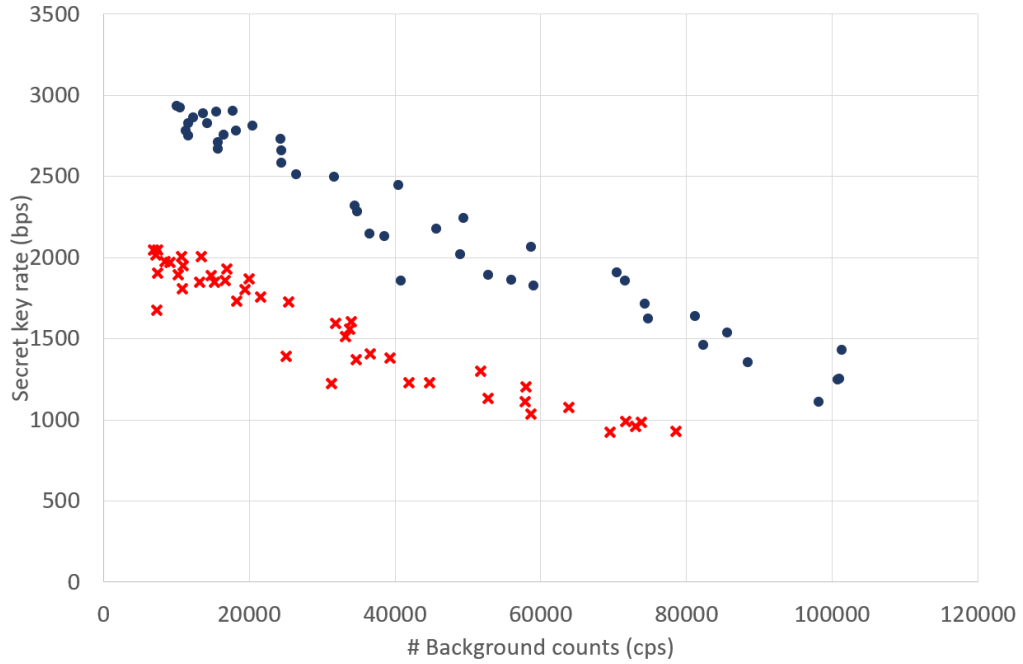


Figure 3. Estimated secret key rate for the original system (blue dots) and with the beamsplitter inserted (red crosses).

4. DISCUSSION

The impact of transmission reduction by adding beamsteering components in the quantum channel was clearly demonstrated leading to reduced secret key rates. Next to the splitting ratio, further reductions of the optical transmission along the optical path inside the receiver cause a decreased signal-to-noise ratio of the QKD signal, and therefore slightly increased error rate. Moreover, the error rate was observed not scale directly with increased transmission losses.

The background light performance shown in this work is intentionally not referenced to an objective measure of the ambient light level. The final beamsteering system will contain several background light reduction schemes, such as reducing the field of view of the receiver, which are not included in the emulation carried out here. The performance of the QKD receiver is expected to be the same for a given level of extraneous counts (which is what is shown in Figs. 2 & 3).

The addition of beamsteering components might reduce the secret key rate by 50%, but they will also enable the seamless integration of untrained users into a QKD network. Future improvements of the hardware could make this impact less significant.

A simplification of a later setup was used for investigations in this contribution. The demonstrated sensitivity to ambient light underlines the need for spatial filtering in a later receiver design.

ACKNOWLEDGMENTS

The presented research was funded by the EPSRC / UKNQTP Quantum Communication Hub (EP/T001011/1).

REFERENCES

- [1] Peev, M., Pacher, C., Alléaume, R., Barreiro, C., Bouda, J., Boxleitner, W., Debuisschert, T., Diamanti, E., Dianati, M., Dynes, J. F., Fasel, S., Fossier, S., Fürst, M., Gautier, J.-D., Gay, O., Gisin, N., Grangier, P., Happe, A., Hasani, Y., Hentschel, M., Hubel, H., Humer, G., Länger, T., Legré, M., Lieger, R., Lodewyck, J., Lorünser, T., Lütkenhaus, N., Marhold, A., Matyus, T., Maurhart, O., Monat, L., Nauerth, S., Page, J.-B., Poppe, A., Querasser, E., Ribordy, G., Robyr, S., Salvail, L., Sharpe, A. W., Shields, A. J., Stucki, D., Suda, M., Tamas, C., Themel, T., Thew, R. T., Thoma, Y., Treiber, A., Trinkler, P., Tualle-Broui, R., Vannel, F., Walenta, N., Weier, H., Weinfurter, H., Wimberger, I., Yuan, Z. L., Zbinden, H., and Zeilinger, A., “The SECOQC quantum key distribution network in vienna,” *New Journal of Physics* **11**, 075001 (jul 2009).
- [2] Sasaki, M., Fujiwara, M., Ishizuka, H., Klaus, W., Wakui, K., Takeoka, M., Miki, S., Yamashita, T., Wang, Z., Tanaka, A., Yoshino, K., Nambu, Y., Takahashi, S., Tajima, A., Tomita, A., Domeki, T., Hasegawa, T., Sakai, Y., Kobayashi, H., Asai, T., Shimizu, K., Tokura, T., Tsurumaru, T., Matsui, M., Honjo, T., Tamaki, K., Takesue, H., Tokura, Y., Dynes, J. F., Dixon, A. R., Sharpe, A. W., Yuan, Z. L., Shields, A. J., Uchikoga, S., Legré, M., Robyr, S., Trinkler, P., Monat, L., Page, J.-B., Ribordy, G., Poppe, A., Allacher, A., Maurhart, O., Länger, T., Peev, M., and Zeilinger, A., “Field test of quantum key distribution in the tokyo QKD network,” *Optics Express* **19**, 10387 (may 2011).
- [3] Mao, Y., Wang, B.-X., Zhao, C., Wang, G., Wang, R., Wang, H., Zhou, F., Nie, J., Chen, Q., Zhao, Y., Zhang, Q., Zhang, J., Chen, T.-Y., and Pan, J.-W., “Integrating quantum key distribution with classical communications in backbone fiber network,” *Optics Express* **26**, 6010 (feb 2018).
- [4] Aguado, A., Hugues-Salas, E., Haigh, P. A., Marhuenda, J., Price, A. B., Sibson, P., Kennard, J. E., Erven, C., Rarity, J. G., Thompson, M. G., Lord, A., Nejabati, R., and Simeonidou, D., “Secure NFV orchestration over an SDN-controlled optical network with time-shared quantum key distribution resources,” *Journal of Lightwave Technology* **35**, 1357–1362 (apr 2017).
- [5] Jennewein, T., Grant, C., Choi, E., Pugh, C., Holloway, C., Bourgoin, J. P., Hakima, H., Higgins, B., and Zee, R., “The NanoQEY mission: Ground to space quantum key and entanglement distribution using a nanosatellite,” in [*Emerging Technologies in Security and Defence II; and Quantum-Physics-based Information Security III*], SPIE (oct 2014).
- [6] Bedington, R., Arrazola, J. M., and Ling, A., “Progress in satellite quantum key distribution,” *npj Quantum Information* **3** (aug 2017).

- [7] Liao, S.-K., Cai, W.-Q., Handsteiner, J., Liu, B., Yin, J., Zhang, L., Rauch, D., Fink, M., Ren, J.-G., Liu, W.-Y., Li, Y., Shen, Q., Cao, Y., Li, F.-Z., Wang, J.-F., Huang, Y.-M., Deng, L., Xi, T., Ma, L., Hu, T., Li, L., Liu, N.-L., Koidl, F., Wang, P., Chen, Y.-A., Wang, X.-B., Steindorfer, M., Kirchner, G., Lu, C.-Y., Shu, R., Ursin, R., Scheidl, T., Peng, C.-Z., Wang, J.-Y., Zeilinger, A., and Pan, J.-W., “Satellite-relayed intercontinental quantum network,” *Physical Review Letters* **120** (jan 2018).
- [8] Polnik, M., Mazzarella, L., Carlo, M. D., Oi, D. K. L., Riccardi, A., and Arulselman, A., “Scheduling of space to ground quantum key distribution,” *EPJ Quantum Technology* **7** (jan 2020).
- [9] Mazzarella, L., Lowe, C., Lowndes, D., Joshi, S. K., Greenland, S., McNeil, D., Mercury, C., Macdonald, M., Rarity, J., and Oi, D. K. L., “QUARC: Quantum research cubesat — a constellation for quantum communication,” *Cryptography* **4**, 7 (feb 2020).
- [10] Lowndes, D., Frick, S., Hart, A., and Rarity, J., “A low cost, short range quantum key distribution system,” *EPJ Quantum Technology* **8**(15) (2021).
- [11] Singh, R., Schreier, A., Faulkner, G., and O’Brien, D., “Fiber-wireless-fiber terminals for optical wireless communication over multiple bands,” in [*2020 IEEE Photonics Conference (IPC)*], 1–2, IEEE (2020).
- [12] Singh, R., Feng, F., Hong, Y., Faulkner, G., Deshmukh, R., Vercasson, G., Bouchet, O., Petropoulos, P., and O’Brien, D., “Design and characterisation of terabit/s capable compact localisation and beam-steering terminals for fiber-wireless-fiber links,” *Journal of Lightwave Technology* **38**(24), 6817–6826 (2020).
- [13] Hong, Y., Feng, F., Bottrill, K. R., Taengnoi, N., Singh, R., Faulkner, G., O’Brien, D. C., and Petropoulos, P., “Beyond terabit/s wdm optical wireless transmission using wavelength-transparent beam tracking and steering,” in [*Optical Fiber Communication Conference*], W1G–4, Optical Society of America (2020).
- [14] Chun, H., Choi, I., Faulkner, G., Clarke, L., Barber, B., George, G., Capon, C., Niskanen, A., Wabnig, J., O’Brien, D., et al., “Handheld free space quantum key distribution with dynamic motion compensation,” *Optics Express* **25**(6), 6784–6795 (2017).
- [15] Ma, X., “Unconditional security at a low cost,” *Physical Review A* **74**(5), 052325 (2006).