Integrated quantum key distribution sender unit for daily-life implementations

Gwenaelle Mélen[a], Tobias Vogl[a], Markus Rau[a], Giacomo Corrielli[b], Andrea Crespi[b], Roberto Osellame[b] and Harald Weinfurter[a,c]

[a] Faculty of Physics, Ludwig-Maximilian-Universität 80799 München, Germany;
[b] Istituto di Fotonica e Nanotecnologie, Consiglio Nazionale delle Ricerche (IFN-CNR) and Dipartimento di Fisica, Politecnico di Milano, 20133 Milano, Italy;
[c] Max-Planck-Institut für Quantenoptik, 85748 Garching bei München, Germany

ABSTRACT

Unlike currently implemented encryption schemes, Quantum Key Distribution provides a secure way of generating and distributing a key among two parties. Although a multitude of research platforms has been developed, the integration of QKD units within classical communication systems remains a tremendous challenge. The recently achieved maturity of integrated photonic technologies could be exploited to create miniature QKD add-ons that could extend the primary function of various existing systems such as mobile devices or optical stations.

In this work we report on an integrated optics module enabling secure short-distance communication for, e.g., quantum access schemes. Using BB84-like protocols, Alice's mobile low-cost device can exchange secure key and information everywhere within a trusted node network. The new optics platform ($35 \times 20 \times 8$ mm) compatible with current smartphone's technology generates NIR faint polarised laser pulses with 100 MHz repetition rate. Fully automated beam tracking and live basis-alignment on Bob's side ensure user-friendly operation with a quantum link efficiency as high as 50 % stable over a few seconds.

Keywords: Quantum Key Distribution, Handheld devices, Smartphone, Integrated optics, Optical transmitters, Vertical-cavity surface-emitting lasers.

1. INTRODUCTION

With the constant increase of data exchanged every day through communication networks, the ability to keep present as well as past transfers of information secure is essential more than ever. As of today, the security of most cryptographic protocols relies on the arbitrarily large amount of computational power required to calculate the key used for encryption and/or decryption. The emergence of quantum computers, expected to solve these mathematical problems within a reasonable amount of time, would allow to decrypt all messages previously encoded based on this type of algorithms. To limit the impact of such breakdown, and to close possible embedded back-doors leaking information to the NSA, scientists have proposed to switch to Quantum Key Distribution[1,2] (QKD)-based protocols. These solutions enable two users, Alice and Bob, to generate a new, random key every time they want to communicate. The single-use of the key, combined with its randomness, makes its reconstruction impossible for an eavesdropper, and its security immune to technological advances. Moreover, QKD exploits the laws of quantum mechanics to guarantee security, and to evaluate the information obtained by a potential eavesdropper during the key generation process.

Most efforts towards practical QKD implementations focus on large-scale networks[3,4] over optical fibres[5] or space-to-ground links,[6,7] although short-distance applications such as card-less payments, network access or the internet of things (IoT) could also benefit from increased security. Miniature add-ons based on photonic nanotechnologies could boost the integration of QKD in mobile devices or in existing optical communication platforms.

Further author information: (Send correspondence to H.W.)
H.W: E-mail: h.w@lmu.de, Telephone: +49 (0)89 2180 2044

Advances in Photonics of Quantum Computing, Memory, and Communication IX, edited by Zameer Ul Hasan, Philip R. Hemmer, Hwang Lee, Alan L. Migdall, Proc. of SPIE Vol. 9762, 97620A
 · doi: 10.1117/12.2208643

In this manuscript we report for the first time a secure key exchange based on the BB84 protocol[8] between a miniature quantum transmitter (Alice, $35 \times 20 \times 8$ mm), possibly integrated in a mobile communication device placed in the hand of a user and a free-space receiver (Bob). To ensure an optical stable link, Bob is equipped with a dynamic alignment system able to track the incoming beam and to adapt its reference-frame depending on the sender's orientation. We first detail the architectures of both apparatus and then present the first proof-of-principle QKD tests showing the performance of the proposed system under realistic experimental conditions.

2. MINIATURE SENDER UNIT

In order to implement BB84-like protocols, Alice needs to produce four different polarisation states forming two mutually unbiased bases, typically $\{|H\rangle, |V\rangle, |+45\rangle, |-45\rangle\}$. These states have to be indistinguishable regarding other degrees of freedom (so-called side-channels) in order to avoid delivering additional information to a potential Eavesdropper (Eve). To achieve this goal with limited footprint and low power consumption, we opt for an architecture based mostly on passive components,[9] as shown in Fig. 1a.

An array of four vertical-cavity surface-emitting lasers (VCSEL) with uniform properties emit weak coherent states at 850 nm. The driving electronics allows to finely tune the bias and modulation currents. The shape and the phase of the pulse can be precisely controlled to achieve excellent temporal overlap between the channels using delay lines with 5 ps resolution. In the strong modulation regime, the 40 ps long optical pulses do not exhibit a well-defined polarisation, therefore enabling the control of each diode by an external polariser. The focused ion beam (FIB) milling technique was used to fabricate an array of four wire-grid polarisers (WGP) with extinction ratios up to 1,800 preparing the four required states.[10] A neutral density filter with $ND = 1.1$ (not shown in Fig. 1a) is placed between the strongly reflecting WGP and the VCSELs to avoid back-injection.

The polarised beams are then coupled via a micro-lens array into a low-birefringence, single-mode waveguide chip where they are combined into one spatial mode. The 3D capability of the femtosecond laser micromachining technique was exploited to create a special 3D layout compensating for intrinsic polarisation effects.[11] Finally, a red beacon laser (680 nm) is overlapped with the infrared signal using a $3.5 \times 3.5 \times 3$ mm dichroic, non-polarising beamsplitter to facilitate the aiming into the receiver and additionally to synchronise both devices. The resulting beam is collimated with a small aspheric lens. To increase the stability of the device, the elements are glued onto a micro-optical bench, as shown in Fig. 1b. The latter is integrated with its driving electronics into a small aluminimium box that will be considered in the following as the handheld Alice device.

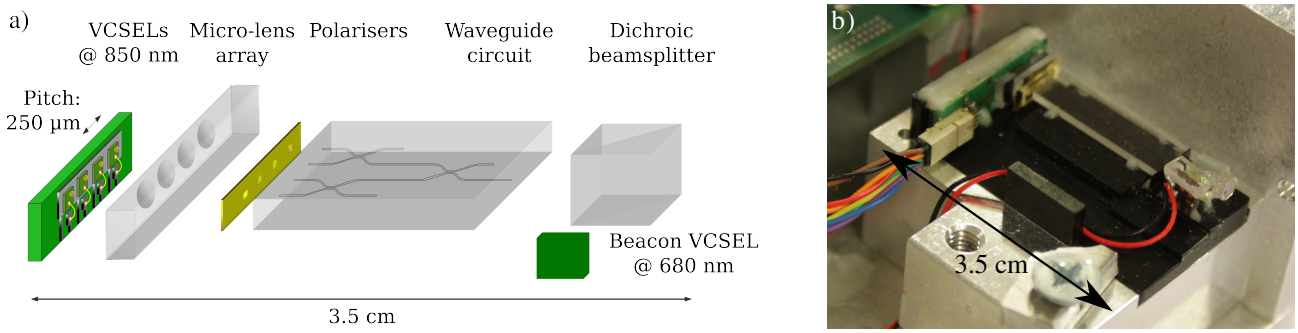

Figure 1. Overview of the integrated Alice architecture. The VCSEL array coupled to a micro-polariser array generates polarised weak coherent states at 850 nm, which are then spatially overlapped in single-mode waveguides micromachined in glass via femtosecond laser writing. The resulting beam is overlapped with a bright visible beacon laser to enable synchronisation and beam tracking on Bob's side. (b) Picture of the resulting module assembled onto a micro-optical bench. The prototype has a size of $35 \times 20 \times 8$ mm.

3. FREE-SPACE RECEIVER

The standard polarisation analysis unit (PAU) used in previous free-space experiments,[6,12] has been extended to achieve a stable optical link and automatic reference frame alignment between both apparatus, as presented in Fig 2. First, the beacon laser, modulated at 100 MHz repetition rate, is split off via a dichroic mirror and detected by a fast photodiode to recover Alice's clock signal. A portion of the visible photons is also focused onto a position-dependent photodiode to determine the aiming angle, which is fed back to a movable mirror. This component adjusts the direction of the infrared beam to ensure a maximum coupling efficiency through the narrow spatial filter and into the detectors. As recently demonstrated,[13] the filter prevents an eavesdropper to exploit the imbalanced detection efficiencies obtained at large incidence angles.

The role of the PAU is then to discriminate between the polarisation states sent by Alice. In this experiment, the latter exhibit an elliptical polarisation due to the small birefringence of the waveguide chip ensuring their spatial indistinguishability. Bob thus rotates the incoming states back to a set of linear polarisations using two quarter-wave plates (QWP) and a half-wave plate (HWP). If the transmitter is slightly tilted in the hand of the user, the preparation and detection bases will not coincide any more, leading to a high quantum bit error ratio (QBER). To allow the user to hold the device in a way he finds comfortable, the whole reference frame is rotated on Bob's side by a motorised half-wave plate (HWP). Assuming that the miniature transmitter can be embedded in a host device such as a smartphone, the tilting angle can be retrieved from the embedded accelerometer and sent to the HWP over WLAN. In the following proof-of-principle tests, the phone is placed on top of the Alice module to fulfil this function, but so far the module itself is connected to a computer.

Finally, the PAU uses a non-polarising beamsplitter to randomly choose the detection basis, and a polarising beamsplitter (PBS) placed in the first arm to separate H and V states. In the second arm, a HWP combined with a PBS allows to distinguish between $\pm 45^o$ states. The photons are detected by actively quenched fibre-coupled avalanche photodiodes (APD) operated in Geiger mode (*SPCM-AQ4C*, Perkin Elmer).

4. FIRST QUANTUM KEY DISTRIBUTION TESTS

For the first test the Alice unit is fixed in front of the receiver, and transmitter and receiver are both connected to a computer, which subsequently analyses the recorded data. As shown in Fig. 3a, an average QBER of 3.3 % was observed under static alignment, with an overall transmission estimated at $t_{link} = 24\,\%$. The lower bound on the achievable (asymptotic) key rate can be calculated using Eq. 1[14]

$$R_{sec} = R_{sift} \cdot \left[(1-\Delta) - f(\delta)\, H_2(\delta) - (1-\Delta)\, H_2\left(\frac{\delta}{1-\Delta}\right) \right] \tag{1}$$

where Δ represents the probability to detect a photon from a multi-photon pulse on Bob's side when an attenuated pulse has been emitted. For an optimal mean photon number $\mu = 0.09$ for this link efficiency, an asymptotic secure key rate of 54 kHz can be achieved, corresponding to a tenfold improvement compared to two other miniaturised sender units with much larger footprints.[15,16]

In a second step, more realistic operation conditions are tested by letting the user hold the transmitter in his hand and aiming into the two entrance pinholes of Bob's set-up at a distance of about 30 cm. The smartphone placed on top of the device records its orientation and communicates with Bob's computer over WLAN. Both dynamic alignment systems should compensate simultaneously for the small lateral displacements and rotations of the sender due to a wobbly hand. The higher transmission loss leads to a higher value of the Δ parameter than in the static case, which can be partially compensated by reducing the mean photon number, in this case down to $\mu = 0.06$. Only the bits exchanged during time intervals where the signal-to-noise ratio is sufficient are considered for the calculation of the QBER and of the secure key rate. Figure 3b shows the results of the first test, yielding an average QBER of 4.1 % and an average secure key rate of 31 Hz.[17]

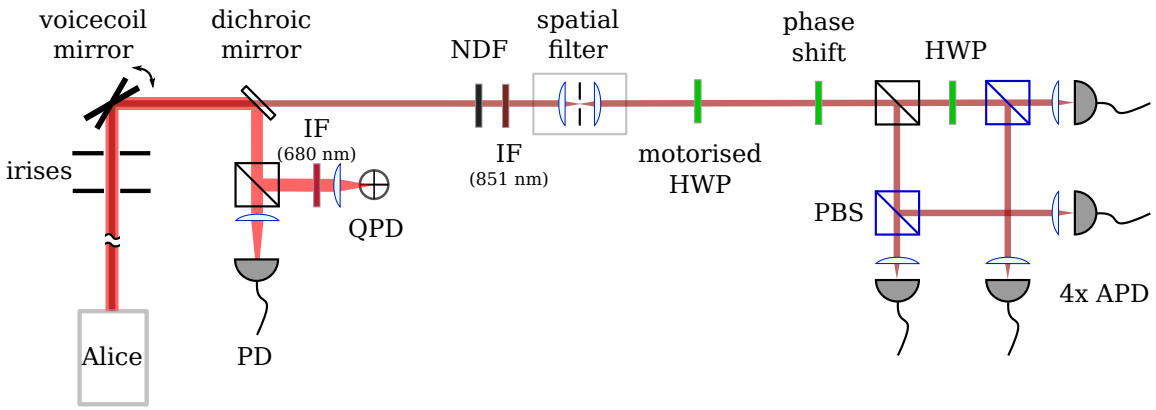

Figure 2. Optical setup of the receiver (Bob). The red beacon laser, overlapped with the polarised qubits, is first detected by a fast photodiode (PD) for synchronisation purposes, and second by a position-sensitive quadrant photodiode (QPD) retrieving the aiming angle. The direction of the beam is corrected by a fast moving voicecoil mirror to ensure a stable detection efficiency. The polarisation states sent by Alice are then analysed as follows: a motorised half-wave plate controlled over WLAN rotates Bob's reference frame in real time, depending on the tilting of the handheld unit. A static phase compensation scheme then rotates the elliptical polarisation states back to linear states, and a first beamsplitter (BS) performs a random basis choice. A polarising beamsplitter (PBS) placed in one arm allows to discriminate between $|H\rangle$ and $|V\rangle$, while a half-wave plate rotated by 22.5^o combined with a PBS in the second arm projects the qubits onto $|D\rangle$ and $|A\rangle$. Technical abbreviations: IF: interference filter; NDF: neutral density filter; HWP: half-wave plate; APD: avalanche photodiode.

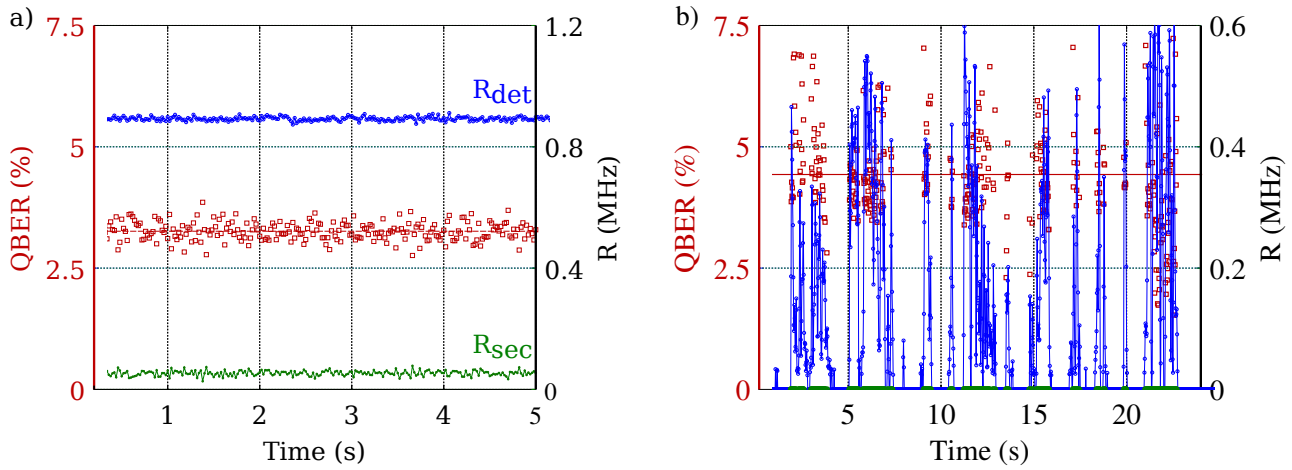

Figure 3. Results of the first QKD tests obtained for (a) static and (b) dynamic alignment between transmitter and receiver. The experiments have been performed with a mean photon number of $\mu = 0.09$ and $\mu = 0.07$, respectively.

5. CONCLUSION

We presented a miniature QKD sender add-on capable of generating polarised weak coherent states at 100 MHz and therefore suitable for the implementation of BB84-like protocols. A dedicated free-space receiver equipped with a dynamic alignment system can track the incoming beam and align its detection bases depending on

the orientation of the transmitter. Under static alignment, a secure key rate of 58 kHz could be achieved with an average QBER of 3.3 %. In a more realistic scenario where the integrated device is held by the user, an average secure key rate of 31 Hz was obtained. Further optimisation of the dynamic alignment systems and of the experimental QKD parameters, together with the implementation of decoy protocols, will enable faster key generation processes, well suited for authentication and short-distance applications in large trusted node networks.

ACKNOWLEDGMENTS

This project was funded by the excellence cluster Nano-Initiative Munich (NIM) and by the European project FP7/QWAD.

REFERENCES

[1] Gisin, N., Ribordy, G., Tittel, W., and Zbinden, H., "Quantum cryptography," *Reviews of Modern Physics* **74**(1), 145–195 (2002).

[2] Lo, H.-K., Curty, M., and Tamaki, K., "Secure quantum key distribution," *Nature Photonics* **8**, 595 (2014).

[3] 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., Hübel, 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-Brouri, 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**(7), 075001 (2009).

[4] 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**(11), 10387–10409 (2011).

[5] Korzh, B., Walenta, N., Lunghi, T., Gisin, N., and Zbinden, H., "Free-running InGaAs single photon detector with 1 dark count per second at 10% efficiency," *Applied Physics Letters* **104**, 081108 (Feb. 2014).

[6] Nauerth, S., Moll, F., Rau, M., Fuchs, C., Horwath, J., Frick, S., and Weinfurter, H., "Air-to-ground quantum communication," *Nature Photonics* **7**, 1–5 (2013).

[7] Vallone, G., Bacco, D., Dequal, D., Gaiarin, S., Luceri, V., Bianco, G., and Villoresi, P., "Experimental Satellite Quantum Communications," *Physical Review Letters* **115**, 040502 (2015).

[8] Bennett, C. H. and Brassard, G., "Quantum cryptography: Public key distribution and coin tossing," in [*Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*], 175–179 (1984).

[9] Vest, G., Rau, M., Fuchs, L., Corrielli, G., Weier, H., Nauerth, S., Crespi, A., Osellame, R., and Weinfurter, H., "Design and evaluation of a handheld quantum key distribution sender module," *IEEE Journal of Selected Topics in Quantum Electronics* **21**(3), 131–137 (2015).

[10] Mélen, G., Rosenfeld, W., and Weinfurter, H., "Impact of the slit geometry on the performance of wire-grid polarisers," *Optics Express* **23**(25), 32171 (2015).

[11] Sansoni, L., Sciarrino, F., Vallone, G., Mataloni, P., Crespi, A., Ramponi, R., and Osellame, R., "Two-Particle Bosonic-Fermionic Quantum Walk via Integrated Photonics," *Physical Review Letters* **108**(1), 1–5 (2012).

[12] Ursin, R., Tiefenbacher, F., Schmitt-Manderbach, T., Weier, H., Scheidl, T., Lindenthal, M., Blauensteiner, B., Jennewein, T., Perdigues, J., Trojek, P., Ömer, B., Fürst, M., Meyenburg, M., Rarity, J., Sodnik, Z., Barbieri, C., Weinfurter, H., and Zeilinger, A., "Entanglement-based quantum communication over 144 km," *Nature Physics* **3**(7), 481–486 (2007).

[13] Rau, M., Vogl, T., Corrielli, G., Vest, G., Fuchs, L., Nauerth, S., and Weinfurter, H., "Spatial mode side channels in free-space QKD implementations," *IEEE Journal of Selected Topics in Quantum Electronics* **21**(3), 1–5 (2015).

[14] Gottesman, D., Lo, H.-K., Lütkenhaus, N., and Preskill, J., "Security of quantum key distribution with imperfect devices," *Quantum Info. Comput.* **4**(5), 325–360 (2004).

[15] Duligall, J. L., Godfrey, M. S., Harrison, K. a., Munro, W. J., and Rarity, J. G., "Low cost and compact quantum key distribution," *New Journal of Physics* **8**(10), 216–249 (2006).

[16] Benton, D., Gorman, P., Tapster, P., and Taylor, D., "A compact free space quantum key distribution system capable of daylight operation," *Optics Communications* **283**(11), 2465–2471 (2010).

[17] For alternative analysis see Vallone, G., Marangon, D. G., Canale, M., Savorgnan, I., Bacco, D., Barbieri, M., Calimani, S., Barbieri, C., Laurenti, N., and Villoresi, P., Adaptive real time selection for quantum key distribution in lossy and turbulent free-space channels, Physical Review A **91** (4), 042320 (2015).