Design and Evaluation of a Handheld Quantum Key Distribution Sender module

Gwenaelle Vest, Markus Rau, Lukas Fuchs, Giacomo Corrielli, Henning Weier, Sebastian Nauerth, Andrea Crespi, Roberto Osellame and Harald Weinfurter

***Abstract*—Currently most Quantum Key Distribution (QKD) experiments are focusing on efficient long-distance implementations. Yet the recent development of miniaturized photonic modules and integrated quantum optics circuits could open new perspectives toward secure short-distance communication for daily-life applications. Here we present the design of a new integrated optics architecture with an effective size of $25 \times 2 \times 1$ mm. Our objective is to obtain an ultra-flat micro-optics QKD add-on suitable for integration into handheld platforms such as smartphones. In this context, we evaluated the suitability of various optical subsystems. We tested an array of four Vertical Cavity Surface Emitting Lasers (VCSEL) with highly similar emission properties capable of producing subnanosecond near-infrared pulses at 100 MHz repetition rate. As short pulses exhibit a low polarization degree, their polarization can be externally controlled by a micro-polarizer array. The fabrication of such elements is quite straightforward using standard lithographic techniques and extinction ratios up to 29 dB have been measured. To guarantee spatial indistinguishability of the qubits, we investigate the option of using low-birefringence, single-mode waveguide array manufactured via femtosecond laser micromachining.**

***Index Terms*—Cryptographic protocols, Quantum Key Distribution, Optical transmitters, Photonic integrated circuits, Three-dimensional integrated circuits, Vertical cavity surface emitting lasers, Microoptics**

I. Introduction

A cryptographic system is known to be only as secure as its key. The security of conventional key generation protocols such as RSA [1] fully relies on the computational complexity to solve some mathematical problems, and as such is seriously threatened by the recent progress towards quantum computers. First introduced thirty years ago, Quantum Key Distribution (QKD) [2], [3] offers an interesting alternative to create and distribute a random key among two parties sharing an initial secret. The laws of quantum physics guarantee security by allowing, for the first time in the history of cryptography, the detection of any leakage of information to an eavesdropper. Commercial stand-alone systems have recently become available, but a progressive transition from classical to quantum communication will require new stable and scalable systems proven to be compatible with standard technologies. Although most efforts are still concentrated on long distance schemes [4], [5], there is an increasing need for an easy-to-operate, portable unit protecting secure daily life authentication processes for *e.g.* banking transactions or towards an upstream quantum access network [6]. In this regard, integrated photonics platforms could enable secure communication with handheld devices such as smartphones. After some initial progress towards this goal [7]–[9], further miniaturization of the components as well as higher key generation rates have to be achieved in order to make pocket-size QKD modules an attractive add-on to conventional wireless methods.

Here we present a new design for a system where one of the users (Alice) owns a mobile QKD-unit which allows her to perform secure free-space communication with, *e.g.*, an ATM or Point-to-Sale machine equipped with the QKD receiver (Bob). A secure key could be generated on demand and either directly used for transactions or stored for future online authentication. Section II introduces the requirements on such a device and compares the performances of diverse architectures. The following sections III-V characterize components for the generation of sub-nanosecond, polarized light pulses and for the spatial overlapping in a waveguide chip. Section VI summarizes the work and discusses possible improvements.

II. Design rules

Several compact QKD sender units have been presented in the past years, demonstrating either high repetition rate or partially miniaturized packaging solutions, but rarely both simultaneously. Our ambition is to achieve a robust and rather flat optical configuration with a few square millimeter footprint in order to fit into, $e.g.$, a smartphone case. The module should run at 100 MHz repetition rate to ensure fast communication and should be driven by simple electronics to enable easy integration into the host's hardware.

While the initial proposal [2] was based on polarization encoding onto single-photons to prevent an eavesdropper to gain knowledge about the key, it has been later demonstrated that theoretical security can be guaranteed even with weak coherent pulses by implementing the decoy state protocol [10]. Attenuated laser pulses are therefore considered appropriate for this project.

The first requirement on the laser is its capability to

Manuscript received August 1, 2014; revised October 6, 2014; accepted October 8, 2014. This work was supported by the EU projects CHIST-ERA/QUASAR, FP7/QWAD and FP7/CIPRIS (MC ITN-287252).

G. Vest, M. Rau, L. Fuchs and H. Weinfurter are with the Faculty of Physics, Ludwig-Maximilian-Universität 80799 München, Germany (e-mail: gwenaelle.vest@lmu.de).

G. Vest, H. Weier and S. Nauerth are with qutools GmbH, 81371 München, Germany.

G. Corrielli, A. Crespi and R. Osellame are with the Istituto di Fotonica e Nanotecnologie, Consiglio Nazionale delle Ricerche (IFN-CNR), and with the Dipartimento di Fisica, Politecnico di Milano, 20133 Milano, Italy.

H. Weinfurter is also with the Max-Planck-Institut für Quantenoptik, 85748 Garching bei München, Germany.

produce pulses that are indistinguishable in the spectral, spatial and time domain. Working with only one source and actively rotating the polarization of each pulse is therefore the most natural strategy in this regard. High modulation speed can be reached with Electro-Optic Modulators (EOM) [11], however usually at the expense of the achievable Quantum Bit Error Rate (QBER) and device dimensions.

Our approach thus consists in using four different attenuated laser sources, each associated with a certain polarization direction. In a previous experiment [12], a small Alice module was implemented with highly polarized edge-emitting diodes in TO cans, overlapped into the quantum channel using a conical mirror. To enhance the scalability, the TO package could simply be removed such that only the bare laser die remains. Unfortunately the generation of the four polarization states $\{H, V, +45, -45\}$ would imply a cumbersome rotation and alignment of the individual diodes. Coupling the light into single-mode waveguides for spatial filtering is also rather inefficient due to the elliptical profile of the modes.

Top emitting sources however, ease the vertical integration with other components and are clearly more suitable for this application. Among them light-emitting diodes (LED) have been considered good candidates for low cost systems [8], [13]. Yet their modulation frequency is limited by the spontaneous emission rate, usually in the nanosecond range, justifying their use for 10 MHz operation but indicating a strong weakness toward upgrading to 100 MHz repetition rate. Vertical Cavity Surface Emitting Lasers (VCSEL), on the other hand, fulfill all the requirements for potential integration into a QKD-system. Their small cavity ensures a single longitudinal mode and hence high coherence length. Neighbouring VCSELs on a single wafer are likely to have uniform emission properties due to highly similar growth conditions, and their standard 250 µm pitch is compatible with other micro-optics elements. Moreover, current technologies reach 40 Gb.s^{-1} modulation speed, and the Laguerre-Gaussian intensity profile guarantees efficient coupling into fibers or waveguides for spatial filtering, suggesting VCSELs as valuable tool.

Nevertheless, an external adjustment of the polarization is necessary to generate the qubits, since all VCSELs within an array exhibit a common optical response. As aforementioned, we concentrate on passive devices, capable of controlling individual diodes, such as an array of micro-polarizers with 250 µm pitch. The strategy consisting in assembling different polarizer sheets results in relatively low orientation accuracy, and can hardly be extended to the sub-millimeter scale. Here we take advantage of nanotechnology fabrication techniques such as Electron-Beam Lithography (EBL) or Focused Ion Beam (FIB) milling to directly produce an array of components preparing the right quantum states. A relevant option is provided by wire-grid polarizers [14], [15]. These sub-wavelength metal gratings act as perfect reflectors for s-polarization (*i.e.* parallel to the stripes) whereas extraordinary transmission occurs for p-polarization due to Surface Plasmon Polariton (SPP) excitation and Fabry-Perot cavity effects at the slit ends [16]. As the filtered polarization is completely reflected, special attention needs to be devoted to avoiding scattering at the interfaces between the optical components or retro-injection into the laser diode.

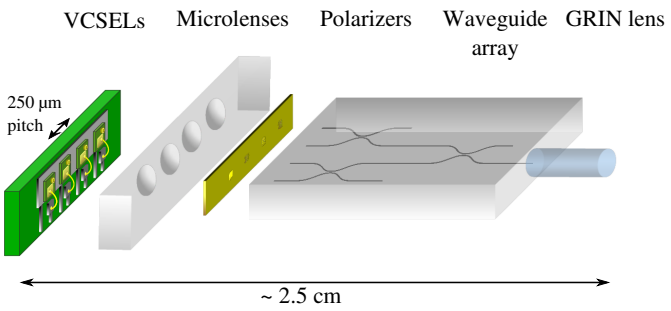

Fig. 1. Overview of the proposed integrated Alice architecture: the 4 VCSELs coupled to micro-polarizers generate the polarization qubits, which are then combined in single-mode waveguides written in borosilicate glass. The effective size is 25 x 2 x 1 mm.

Additionally, spatial filtering methods should also be investigated. In view of compactness as well as mechanical and thermal stability we focus on single-mode, low birefringence waveguide arrays rather than optical fibers. Lithographically fabricated Photonic Integrated Circuits (PIC) benefit from the mature industrial development of the semiconductor technology, reaching high integration density and low propagation losses. Whereas they have been used to demonstrate the first on-chip qubit manipulations [17], [18], they do not sustain polarization encoding due to waveguide birefringence and their layout is restricted to planar configurations. These limitations can be overcome by the femtosecond laser writing technique [19], [20], which has recently emerged as a fast, single-step alternative fabrication method allowing three-dimensional photonic architectures [21], [22].

The resulting arrangement of our prototype is shown in Figure 1. An array of four VCSELs emit synchronized picosecond optical pulses at 100 MHz repetition rate. The polarization state of each diode is controlled by an external array of four wire-grid micro-polarizers fabricated by FIB milling. The four polarized beams are coupled into a waveguide chip and combined to one main output via three polarization independent directional couplers.

III. Generation of faint unpolarized laser pulses

The first component under evaluation is a commercial multi-mode VCSEL array from VI Systems emitting light around 858 nm and engineered for 28 Gb.s^{-1} operation [23]. Single-mode VCSELs would be preferable but arrays are unfortunately not on the market yet. For the characterization, the chips are glued and wire-bonded onto a small thermally stabilized PCB. Each diode is independently driven either in continuous or in pulsed mode, at 100 MHz repetition rate. In each of the four channels, electrical pulses are generated with standard logic gates and synchronized using delay lines with 10 ps resolution. A FPGA allows for fast switching between

the diodes following either a fixed or a random pattern. The bias (DC) and modulation (AC) currents of each VCSEL are regulated by a driver chip and all the parameters can be changed on the fly via a USB connection.

The VCSELs were first characterized in the CW regime. They were collimated with an aspheric lens ($f = 4\,\text{mm}$) and the emitted light power was recorded as a function of the injected current (L-I curve) with a powermeter (Thorlabs, PM100). The threshold current was found to be around 0.95 mA, with 3 % uniformity across the array.

The polarization properties were analyzed using a quarter-wave plate and a polarizer. The Degree of Polarization (DOP) as well as the polarization state could then be reconstructed from the Stokes vector measurements.

The polarization features of VCSELs are generally hard to predict. Even though the gain medium is isotropic and the aperture is circular, experience showed that only two linear modes polarized along orthogonal directions ([110] and [$\bar{1}$10] in GaAs) can lase. This symmetry breaking seems to be mainly associated with intrinsic strain birefringence in the layers as well as electro-optical effects during operation [24]. In our case, the diodes are mostly polarized along H with a DOP around 90 % in CW mode, and no polarization switching was observed over the whole current range (0-16 mA).

For pulsed mode a strong modulation I_m is superimposed on a constant bias current I_b, which should be maintained well below the threshold to obtain high signal to noise ratio. A trade-off has to be found for the DC part to ensure both low spontaneous emission rate (low values) and fast switching times guaranteed by a certain level of carrier density in the active layer (high values). Although the polarization behavior is not well documented in this regime, it has been observed that a steady state is not reached instantaneously after turn-on. The evolution of the DOP with the pulse length was hence characterized, and the values of both currents were optimized to obtain the highest on/off contrast as well as a polarization-independent pulse shape. The optical pulses could be directly visualized using a 9 GHz amplified GaAs photodiode connected to a 20 GHz sampling oscilloscope (Agilent). A Single-photon Avalanche PhotoDiode (SAPD) with 30 ps jitter also enabled to retrieve the pulse shape from the time-difference histogram between the APD pulses and the 100 MHz trigger of the electronic board.

As a starting point we chose an electrical pulse length of 1 ns. As depicted in Figure 2a, the emission is still mostly polarized along H within the optical pulse, and the DOP is close to 90 %, as in CW operation. The carrier relaxation phenomenon is clearly visible, and the results suggest that a different polarization behavior arises during the first oscillation. By decreasing the pulse length down to this region, the DOP could be reduced down to 34 % for $I_b = 0.95\,\text{mA}$, $I_m = 15\,\text{mA}$. The final configuration, where each chip is associated with a certain polarization, was reproduced by measuring each diode independently with a fixed polarizer along the path. As the emission along H was still twice as large as along V, a tuning of each diode was necessary to match the intensities after the polarizers with different orientations.

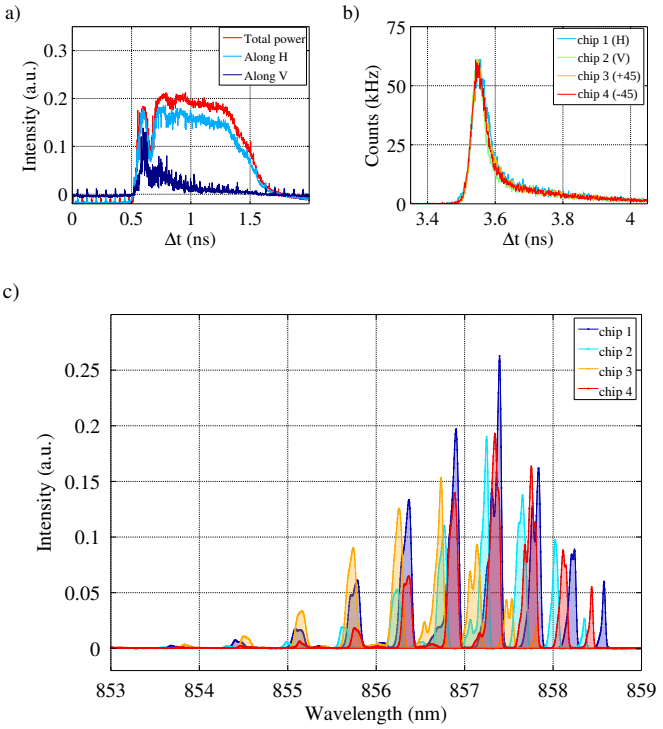

Fig. 2. Characterization of the optical pulses emitted by the VCSEL array. a) Polarization-resolved temporal profile of a long pulse. A steady-state is reached after 0.5 ns, whereas the first part of the pulse exhibits a low DOP. b) Tuning of the electrical pulses allows for synchronization between the four channels, as well as an identical temporal shape even after different polarizers. Here the chips 1,2,3,4 are measured along $\{H, V, +45, -45\}$, respectively. c) FTIR spectrum of the four optimized subnanosecond pulses presented in b). The transverse modes are clearly visible.

The parameters of the driving electronics could be adjusted to obtain perfect intensity and temporal overlap for the four channels (Fig. 2b). In this configuration, the calculated mean photon number per pulse was $\mu = 3.10^6$. As an attenuation of 10^8 was used for the measurement, a Poissonian distribution of the detected photons at the output of the sender is expected. In the final device, μ will be set according to the protocol first in a coarse way using neutral density filters and then in a finer way by tuning the modulation current.

The on/off ratio measured with the raw countrate was around 20 dB for all the VCSELs, but could be clearly increased by reducing the size of the detection window (*e.g.* 30 dB for a 400 ps long gating). The spectral properties of the pulses were measured with a FTIR spectrometer (Vertex 70, Brucker). The thermal shift was estimated at $\Delta\lambda = 0.06\,\text{nm.K}^{-1}$. and a comparison of the chips is presented in Figure 2c. Evidently, the spectral separation of the fundamental modes of the chips ($(\Delta\lambda)_{max} \approx 0.8\,\text{nm}$) has to be compensated in a future version either by thermal tuning of individual diodes or by using MEMS tunable VCSELs [25].

IV. Polarization State Control

To generate the qubits, the optical pulses emanating from each VCSEL have to be passively polarized. We chose to fabricate a wire-grid polarizer array by engraving

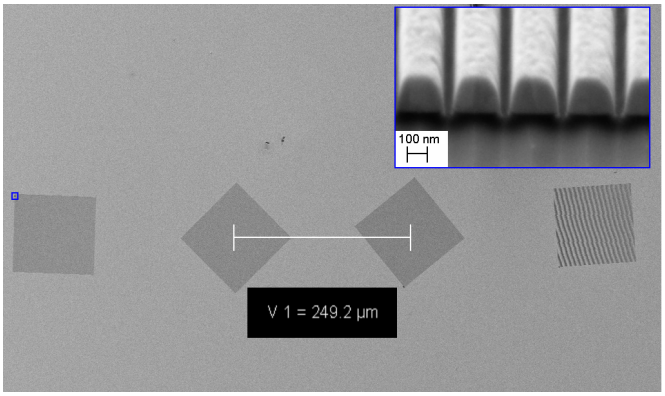

Fig. 3. Array of four 120 × 120 µm wire-grid polarizers with 250 µm pitch fabricated by Focused Ion Beam milling. Inset: Cross-section of the gold stripes.

sub-wavelength gratings into a gold layer via FIB milling. This manufacturing method results in high relative orientation accuracy, compared to assembling different polarizer sheets or rotating polarized laser diodes, as seen in other compact units. The challenge consists in obtaining metal stripes with a rectangular and smooth cross-section, due to a severe dependence of the stripe profile with the polarizing efficiency, and in achieving high reproducibility of the ion beam focusing.

The geometrical parameters of the gratings were optimized with Finite-Difference Time-Domain (FDTD) simulations [26]. The extinction ratio reaches a maximum for an optimal thickness, due to a resonant excitation of the Fabry-Perot cavity formed at the slit ends, whereas thinner slits always result in higher polarization filtering, but lower transmission. Both parameters can be jointly optimized [27], but the minimum achievable slit width is limited by current nano-patterning techniques through thick films (a few hundreds of nanometers). A good compromise is achieved with a 265 nm thick gold layer, 150 nm wide slits and a 500 nm period. Since the polarization splitting mechanism is based on reflection, optical simulations (ZEMAX) were also conducted to evaluate the retro-injection probability of this reflected beam into the diodes. VCSELs are in fact known to be sensitive to optical injection, which can lead to strong modulation of the emitted pulse in the intensity as well as in the polarization degree of freedom. As a back-coupling efficiency close to 0.4 % was predicted for our arrangement, a thin neutral density filter (OD = 1) is intended to be placed in the final module between the micro-lenses and the gold surface to limit this effect as far as possible.

A 120 × 120 µm wire-grid polarizer array with 250 µm pitch was fabricated on top of a thin glass substrate and Scanning-Electron Microscope (SEM) pictures of the polarizer matrix are presented in Figure 3. Extinction ratios of up to 29 dB could be measured (Table I), although the fabrication of four equally performing polarizers remains difficult. As predicted by the simulations, all polarizers feature a transmission close to 9 % and a reflection around 20 % for the p-polarization.

TABLE I
PERFORMANCES OF THE MICRO-POLARIZER ARRAY

Polarizer	1 (H')	2 (+ 45')	3 (− 45')	4 (V')
Extinction Ratio	1:380	1:650	1:720	1:850
QBER (%)	0.26	0.15	0.14	0.12

V. ENSURING SPATIAL OVERLAP OF THE QUBITS

Finally, the initial spatial distinguishability of the pulses has to be addressed. For polarization encoding femtosecond laser micromachining promises the best performance, as it allows to realize 3D low-birefringence waveguide-based optical circuits in a fast and direct manner. The device under test was therefore fabricated using this technique. Here a train of ultrashort (≈ 400 fs) laser pulses at $\lambda = 1040$ nm, produced by a regeneratively amplified Yb-based laser (High-Qlaser FEMTORegen), at the repetition rate of 960 kHz and with an energy of 280 nJ/pulse was focused into an alumino-boro-silicate glass substrate (EAGLE2000, from Corning Inc.) by means of a microscope objective ($NA = 0.6$, 50 x magnification). Single mode optical waveguides for light at 850 nm, with relatively small propagation loss (≈ 0.5 dB.cm^{-1}) could be fabricated by translating the substrate at the constant speed of 43 mm.s^{-1}.

The waveguides manufactured using this technique exhibit a slight degree of birefringence ($\Delta n = 7.10^{-5}$), with the optical axes defined by the fabricating laser beam direction (usually vertical). This causes some dependence of the propagation of light on its polarization state. In particular, the dimensions of the transverse mode profile, measured by near field imaging at the waveguide output facet, were found to be 4×4.7 µm^2 for horizontally polarized light and 3.8×4.8 µm^2 for vertically polarized light. The overlap between the measured mode profiles is as high as 99 %.

The structure of the spatial mode mixer circuit is depicted in Figure 4a. It is composed of three identical 50:50 directional couplers, enabling the photons injected in each of the four input ports (250 µm pitch) to have the same probability to come out from the main output of the device. In order to minimize the polarization dependence of the circuit, a special 3D geometry was employed in the design of the directional couplers [28], in which the evanescent interaction in the waveguides' coupling region takes place with a certain angle θ out of the circuit plane. The radius of curvature R of the bent parts was carefully chosen in order to minimize the polarization dependence of the bending losses (which increase for smaller values of R) while guaranteeing a minimum footprint of the device. The optimum value of $R = 45$ mm, adopted for the circuit fabrication, yields losses of 0.31 dB.cm^{-1} for V and 0.33 dB.cm^{-1} for H. Choosing the interaction length $L = 450$ µm , the waveguide coupling distance $d = 7$ µm and the angle $\theta = 58^o$, it was possible to obtain 50 : 50 directional couplers with a polarization dependence of the splitting ratio below 1 %. Figure 4 shows how the three secondary output arms of the device are bent away from the main one, in order to reduce as much as

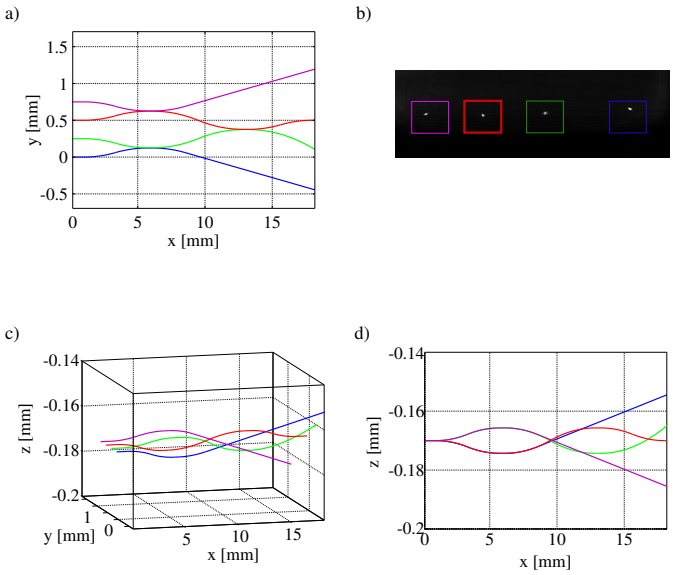

Fig. 4. Three-dimensional waveguide architecture to combine the four beams into one main output (red curve). The three other outputs are deflected both vertically and horizontally. a),c),d) Top, main and side view of the circuit. b) Imaging of the output facet of the circuit when the four VCSELs are coupled into the four waveguides via micro-lenses.

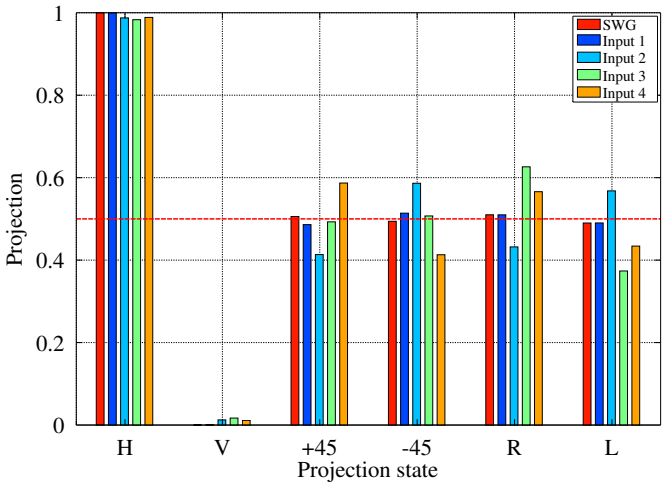

Fig. 5. Projection measurements of the output state when H-polarized light is injected into each of the four inputs of the photonic circuit. The behavior of a straight waveguide is shown for comparison (red)

TABLE II
OPTIMUM LINEAR INPUT STATES CALCULATED BY INVERTING THE MÜLLER MATRIX OF EACH INPUT PORT

Input port	1	2	3	4
Input State	-0.95^o	-43.86^o	39.94^o	86.76^o
Output state	H'	$+45$'	-45'	V'

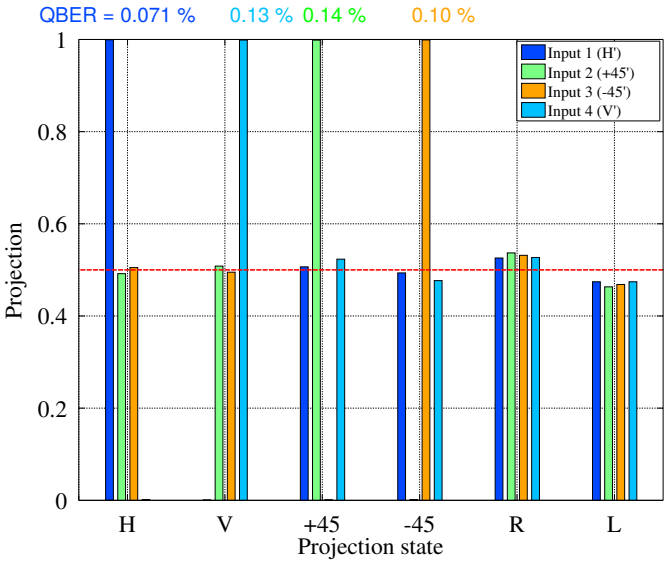

Fig. 6. Reconstructed tomography of these optimal output states, $i.e.$ when $\{H', +45', -45', V'\}$ are launched into the inputs $\{1, 2, 3, 4\}$ respectively.

possible the noise contribution in the photon transmission.

To verify the polarization transformation of the states after the propagation through the circuit, a full process tomography measurement was performed, from which the Müller matrices describing the action of the four device channels were retrieved. This analysis highlighted that a small rotation of the polarization takes place in the circuit, even for linear input states aligned with the waveguides birefringence axes. Figure 5 compares the tomography performed at the output of a straight waveguide (red column) and at the main circuit output (each color corresponds to a different input port), when horizontally polarized light is used as the input state. The H polarization state is not affected by propagating through the straight waveguide, while it gets rotated when propagating through the circuit. This effect could be explained by a local alteration of the birefringence direction caused by the high proximity of the waveguides in the coupling regions, at a certain angle. In fact, as demonstrated recently [29], the stress field that surrounds a waveguide can strongly influence the birefringence of the neighboring ones and possibly causes a rotation of the optical axis, depending on their relative position. In order to compensate for this effect, we used the measured Müller matrices to numerically compute the optimum linear input states that produce the minimum possible QBER (projection onto the eigenbasis) while maintaining pairwise orthogonal output states, after an additional external phase compensation either on Alice or on Bob side. This effect was taken into account beforehand in the fabrication of the micro-polarizers, which produce these optimal states. The optimization results shown in Figure 6 also take into account a phase compensation of $\approx \pi/6$ rad. QBERs smaller than 0.15 % can be achieved, proving the correction for residual birefringence in the waveguides possible.

The remaining imperfections in the output states may result in an imbalanced choice in the basis or in the bit value. This effect can be reduced by fine tuning the pulse intensities and hence the probability of each outcome. Additionally, a loss [30] or a basis symmetrization protocol [31], [32] could be implemented. Alternatively, a device quality q [33] of the

ensemble of generated states

$$q = -log_2 \left[\max_{(\psi_x, \psi_z)} \left(|\langle \psi_x \mid \psi_z \rangle|^2 \right) \right] \quad (1)$$

can be defined. The value $q = 1$ is obtained for perfectly conjugated bases ψ_x and ψ_z. If $q = 0$, two states of the different bases perfectly overlap, and Eve can perform an intercept-resend attack where she always measures along this direction. This allows her to gain full information about the key while remaining completely invisible. In our case, the optimal states presented in Table II yield $q = 0.92$. Using the security analysis given in [33], this device quality leads to a reduction of the secret key rate of 8 %.

VI. Conclusion

We showed that 100 ps faint laser pulses can be generated at 100 MHz repetition rate by an array of four VCSELs. The electrical pulses can be tuned independently for each channel to achieve short optical pulses with an excellent time overlap and exhibiting a low degree of polarization. A pulse length of around 100 ps could be achieved, leading to a signal-to-noise ratio of 30 dB for a 400 ps long detection window. To close the side-channel related to the distinguishability in the spectral domain, the multi-mode VCSELs will be replaced in a future version by their single-mode counterpart, and an individual compensation of the thermal shift via (electro)-thermal tuning of the diodes will be required.

We also demonstrated that the polarization states can be externally generated by an array of four wire-grid micro-polarizers fabricated by Focused Ion Beam milling. Finally, the spatial overlap of the four polarization qubits can be guaranteed by coupling the beams into a waveguide chip and combining them into one main output via three directional couplers. Although the design was engineered to obtain a polarization independent behavior, a slight additional birefringence was observed but could be compensated by rotating the input states in order to ensure low QBERs as well as orthogonality of the resulting bases. This effect could be reduced in the next prototype by carefully optimizing the distance between the arms of the directional couplers, eliminating the need to produce a specific polarizers array for each waveguide chip.

As confirmed in a test assembly, the micro-optics components can be precisely aligned using micro-positioners and NIR-cameras. The final micro-optics device can be as small as 25 × 2 × 1 mm. The driving electronics is made of standard off-the-shelf components and could be easily monolithically integrated into handheld hardware. Whereas more investigation of the complete module is needed, the evaluated micro-optics components form a promising basis for short-range, free-space QKD applications.

Acknowledgment

G.V. thanks Philipp Altpeter (LMU), Peter Weiser and Sonja Matich (WSI) for the technical support with clean room processes, Guilhem Almuneau (LAAS) for interesting discussion on VCSEL properties and Nathalie Picqué (MPQ) for assistance with the spectrum measurements.

References

[1] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, 1978. [Online]. Available: http://dl.acm.org/citation.cfm?id=359342

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

[3] N. Gisin, G. Ribordy, and H. Zbinden, "Quantum cryptography," *arXiv preprint quant-ph/0101098*, vol. 74, no. January, pp. 145–195, 2001. [Online]. Available: http://arxiv.org/abs/quantph/0101098

[4] S. Nauerth, F. Moll, M. Rau, C. Fuchs, J. Horwath, S. Frick, and H. Weinfurter, "Air-to-ground quantum communication," *Nature Photonics*, no. March, pp. 1–5, 2013. [Online]. Available: http://dx.doi.org/10.1038/nphoton.2013.46

[5] J. Wang, B. Yang, S. Liao, L. Zhang, and Q. Shen, "Direct and full-scale experimental verifications towards ground-satellite quantum key distribution," *Nature Photonics*, vol. 7, no. April, pp. 387–393, 2013. [Online]. Available: http://www.nature.com/nphoton/journal/v7/n5/abs/nphoton.2013.89.html

[6] B. Fröhlich, J. Dynes, M. Lucamarini, A. W. Sharpe, Z. Yuan, and A. J. Shields, "A quantum access network," *Nature*, vol. 501, pp. 69–73, 2013. [Online]. Available: http://www.nature.com/nature/journal/v501/n7465/abs/nature12493.html

[7] J. L. Duligall, M. S. Godfrey, K. A. Harrison, W. J. Munro, and J. G. Rarity, "Low cost and compact quantum key distribution," *New Journal of Physics*, vol. 8, no. 10, p. 249, 2006. [Online]. Available: http://stacks.iop.org/1367-2630/8/i=10/a=249

[8] D. Benton, P. Gorman, P. Tapster, and D. Taylor, "A compact free space quantum key distribution system capable of daylight operation," *Optics Communications*, vol. 283, no. 11, pp. 2465–2471, 2010. [Online]. Available: http://dx.doi.org/10.1016/j.optcom.2009.10.039http://www.sciencedirect.com/science/article/pii/S0030401809010141

[9] R. Pizzi, D. Rossetti, and D. D'Arenzo, "Affordable Quantum Cryptography System for Mobile Devices," *International journal of computer ...*, vol. 2, no. 4, pp. 1052–1054, 2012. [Online]. Available: http://www.dti.unimi.it/pizzi/paperi/crypto.pdf

[10] W.-Y. Hwang, "Quantum Key Distribution with High Loss: Toward Global Secure Communication," *Physical Review Letters*, vol. 91, no. 5, pp. 1–4, Aug. 2003. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevLett.91.057901

[11] M. Rau, T. Heindel, and S. Unsleber, "Free space quantum key distribution over 500 meters using electrically driven quantum dot single-photon sourcesa proof of principle experiment," *New Journal of ...*, vol. 043003, 2014. [Online]. Available: http://iopscience.iop.org/1367-2630/16/4/043003

[12] T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, A. Zeilinger, and H. Weinfurter, "Experimental demonstration of free-space decoy-state quantum key distribution over 144 km," *Physical Review Letters*, vol. 010504, no. January, 2007. [Online]. Available: http://journals.aps.org/prl/abstract/10.1103/PhysRevLett.98.010504

[13] J. L. Duligall, M. S. Godfrey, K. a. Harrison, W. J. Munro, and J. G. Rarity, "Low cost and compact quantum key distribution," *New Journal of Physics*, vol. 8, no. 10, pp. 249–249, Oct. 2006. [Online]. Available: http://stacks.iop.org/1367-2630/8/i=10/a=249?key=crossref.d437c7617f9d6c1588a3dcda265b233a

[14] M. Guillaumée, L. Dunbar, C. Santschi, E. Grenet, and R. Eckert, "Polarization sensitive silicon photodiodes using nanostructured metallic grids," *Applied Physics Letters*, vol. 28, no. 6, 2009. [Online]. Available: http://scitation.aip.org/content/aip/journal/apl/94/19/10.1063/1.3133862

[15] H. Tamada, T. Doumuki, T. Yamaguchi, and S. Matsumoto, "Al wire-grid polarizer using the," vol. 22, no. 6, pp. 419–421, 1997.

[16] M. Guillaumée, L. A. Dunbar, C. Santschi, E. Grenet, R. Eckert, O. J. F. Martin, and R. P. Stanley, "Polarization sensitive silicon photodiodes using nanostructured metallic grids," *Applied Physics Letters*, vol. 94, no. 19, pp. –, 2009. [Online]. Available: http://scitation.aip.org/content/aip/journal/apl/94/19/10.1063/1.3133862

[17] J. Matthews, A. Politi, A. Stefanov, and J. O'Brien, "Manipulation of multiphoton entanglement in waveguide quantum circuits," *Nature Photonics*, vol. 3, no. June, 2009. [Online]. Available: http://www.nature.com/nphoton/journal/v3/n6/abs/nphoton.2009.93.html

[18] J. Silverstone, D. Bonneau, and K. Ohira, "On-chip quantum interference between silicon photon-pair sources," *Nature* ..., no. December, pp. 2–6, 2013. [Online]. Available: http://dx.doi.org/10.1038/nphoton.2013.339http://www.nature.com/nphoton/journal/vaop/ncurrent/full/nphoton.2013.339.html

[19] K. M. Davis, K. Miura, N. Sugimoto, and K. Hirao, "Writing waveguides in glass with a femtosecond laser." *Optics letters*, vol. 21, no. 21, pp. 1729–31, Nov. 1996. [Online]. Available: http://www.ncbi.nlm.nih.gov/pubmed/19881782

[20] G. Della Valle, R. Osellame, and P. Laporta, "Micromachining of photonic devices by femtosecond laser pulses," *Journal of Optics A: Pure and Applied Optics*, vol. 11, no. 1, p. 13001, 2009. [Online]. Available: http://iopscience.iop.org/1464-4258/11/1/013001

[21] A. Crespi, R. Ramponi, R. Osellame, L. Sansoni, I. Bongioanni, F. Sciarrino, G. Vallone, and P. Mataloni, "Integrated photonic quantum gates for polarization qubits," *Nature Communications*, vol. 2, p. 566, Nov. 2011. [Online]. Available: http://www.nature.com/doifinder/10.1038/ncomms1570

[22] R. Keil, M. Heinrich, F. Dreisow, T. Pertsch, A. Tünnermann, S. Nolte, D. N. Christodoulides, and A. Szameit, "All-optical routing and switching for three-dimensional photonic circuitry." *Scientific reports*, vol. 1, p. 94, Jan. 2011. [Online]. Available: http://www.pubmedcentral.nih.gov/articlerender.fcgi?artid=3216580\&tool=pmcentrez\&rendertype=abstract

[23] L. Y. Karachinsky, S. A. Blokhin, I. I. Novikov, N. A. Maleev, A. G. Kuzmenkov, M. A. Bobrov, J. A. Lott, N. N. Ledentsov, V. A. Shchukin, J.-R. Kropp, and D. Bimberg, "Reliability performance of 25 Gbit s 1 850 nm vertical-cavity surface-emitting lasers," *Semiconductor Science and Technology*, vol. 28, no. 6, p. 65010, 2013. [Online]. Available: http://stacks.iop.org/0268-1242/28/i=6/a=065010

[24] R. Michalzik, *VCSELs: Fundamentals, Technology and Applications of Vertical-Cavity Surface-Emitting Lasers*, ser. Springer Series in Optical Sciences, R. Michalzik, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, vol. 166. [Online]. Available: http://link.springer.com/10.1007/978-3-642-24986-0

[25] H. a. Davani, B. Kögel, P. Debernardi, C. Grasse, C. Gierl, K. Zogal, A. Haglund, J. Gustavsson, P. Westbergh, T. Gründl, P. Komissinskiy, T. Bitsch, L. Alff, F. Küppers, a. Larsson, M.-C. Amann, and P. Meissner, "Polarization investigation of a tunable high-speed short-wavelength bulk-micromachined MEMS-VCSEL," p. 82760T, 2012. [Online]. Available: http://proceedings.spiedigitallibrary.org/proceeding.aspx?doi=10.1117/12.908262

[26] A. F. Oskooi, D. Roundy, M. Ibanescu, P. Bermel, J. D. Joannopoulos, and S. G. Johnson, "MEEP: A flexible free-software package for electromagnetic simulations by the FDTD method," *Computer Physics Communications*, vol. 181, pp. 687—-702, 2010.

[27] a. T. M. A. Rahman, P. Majewski, and K. Vasilev, "Extraordinary optical transmission: coupling of the Wood-Rayleigh anomaly and the Fabry-Perot resonance." *Optics letters*, vol. 37, no. 10, pp. 1742–4, May 2012. [Online]. Available: http://www.ncbi.nlm.nih.gov/pubmed/22627556

[28] L. Sansoni, F. Sciarrino, G. Vallone, P. Mataloni, A. Crespi, R. Ramponi, and R. Osellame, "Two-Particle Bosonic-Fermionic Quantum Walk via Integrated Photonics," *Physical Review Letters*, vol. 108, no. 1, pp. 1–5, Jan. 2012. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevLett.108.010502

[29] R. Heilmann, M. Gräfe, S. Nolte, and A. Szameit, "Arbitrary photonic wave plate operations on chip: realizing Hadamard, Pauli-X, and rotation gates for polarisation qubits." *Scientific reports*, vol. 4, p. 4118, Jan. 2014. [Online]. Available: http://www.pubmedcentral.nih.gov/articlerender.fcgi?artid=3927208\&tool=pmcentrez\&rendertype=abstract

[30] N. H. Y. Ng, S. K. Joshi, C. C. Ming, C. Kurtsiefer, and S. Wehner, "Experimental implementation of bit commitment in the noisy-storage model." *Nature communications*, vol. 3, no. May, p. 1326, Jan. 2012. [Online]. Available: http://www.ncbi.nlm.nih.gov/pubmed/23271659

[31] H.-K. Lo, H. Chau, and M. Ardehali, "Efficient Quantum Key Distribution Scheme and a Proof of Its Unconditional Security," *Journal of Cryptology*, vol. 18, no. 2, pp. 133–165, Mar. 2004. [Online]. Available: http://link.springer.com/10.1007/s00145-004-0142-y

[32] C. Erven, X. Ma, R. Laflamme, and G. Weihs, "Entangled quantum key distribution with a biased basis choice," *New Journal of Physics*, vol. 11, no. 4, p. 045025, Apr. 2009. [Online]. Available: http://stacks.iop.org/1367-2630/11/i=4/a=045025?key=crossref.711de83b7417cc32171f7bd736231622

[33] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, "Tight finite-key analysis for quantum cryptography." *Nature communications*, vol. 3, no. may 2011, p. 634, Jan. 2012. [Online]. Available: http://www.pubmedcentral.nih.gov/articlerender.fcgi?artid=3274703\&tool=pmcentrez\&rendertype=abstract

Gwenaelle Vest graduated in Materials Engineering from the National Institute of Applied Sciences of Lyon (INSA Lyon), France, in 2011 and in Nanotechnologies from the Université de Lyon, France the same year.

Ms. Vest is now with qutools GmbH. Concurrently, she is working toward a Ph.D. degree in Physics at the Ludwig-Maximilians-Universität (LMU) in Munich, Germany. Her project focuses on high-speed, handheld Quantum Key Distribution modules .

Markus Rau graduated 2008 at the Ludwig-Maximilians-Universität (LMU) in Munich in physics. He is currently a Ph.D. student in the group of Harald Weinfurter. His research interests include QKD with single photon sources and the security of QKD systems.

Lukas Fuchs received his B.Sc. in Physics at the LMU in Munich, Germany in 2012. He is currently pursuing a M.Sc degree at the same university and his thesis focuses on integrated Quantum Key Distribution modules.

Giacomo Corrielli was born in 1986, graduated in Physics Engineering at Politecnico of Milano in 2011 with a thesis concerning the frequency conversion of single photons for quantum repeater applications developed at ICFO, Barcelona.

He is currently Ph.D. student at Politecnico of Milano and his research interests are related to the fabrication of integrated optical circuits for quantum optics and quantum information application.

Henning Weier graduated in Physics on Experimental Quantum Cryptography at the Technische Universität München, Germany in 2003. Dr. Weier received his Ph.D from Ludwig-Maximilians-Universität München, Germany in 2005, his thesis being entitled "Experimental Quantum Key Distribution Network".

In 2005, he co-founded the SME qutools GmbH where he has been CEO ever since.

Sebastian Nauerth graduated in Physics from the Ludwig-Maximilians-Universität München, Germany in 2007, after completing his thesis on free-space quantum key distribution. His doctoral thesis focused on "Air to Ground Quantum Key Distribution" and he obtained his Ph.D. degree from the same university in 2013.

Since 2013, Dr. Nauerth is R&D engineer at qutools GmbH.

Andrea Crespi studied at Politecnico di Milano, obtaining the Master Degree in Engineering Physics in 2008 and the PhD in Physics in 2012.

He is currently working as post-doc fellow at Istituto di Fotonica e Nanotecnologie - Consiglio Nazionale delle Ricerche, in Milano. His current research interests concern development of integrated photonic circuits for sensing and for quantum information applications.

Roberto Osellame received the Laurea degree in electronic engineering from the Politecnico di Milano, Milan, Italy, in 1996, and the Ph.D. degree in physics from the Politecnico di Torino, Turin, Italy, in 2000.

Since 2001, he has been a Research Associate with the Institute of Photonics and Nanotechnologies (IFN), Milan, Italy, of the Italian National Research Council (CNR). He is also currently a Contract Professor at the Politecnico di Milano, teaching experimental physics in the Faculty of Engineering. His research interests include integrated all-optical devices on nonlinear crystals and femtosecond laser writing of active and passive waveguides on glasses.

Prof. Osellame is a member of the Optical Society of America.

Harald Weinfurter received the Diploma and the Ph.D. degree in neutron optics experiments from the Technical University of Vienna, Vienna, Austria, the latter in 1987.

Prof. Weinfurter was a Postdoctoral Fellow at the Hahn-Meitner Institut, Berlin, Germany, and the RISØ-Laboratory, Roskilde, Denmark. In 1991, he started working on foundations of quantum physics and quantum information at the University of Innsbruck, Austria, in the group of Anton Zeilinger. In 1999, he became a member of the Faculty of Physics, University of Munich. He is currently with the Max-Planck-Institute of Quantum Optics (MPQ), Garching, Germany, and with the Department for Physics, Ludwig-Maximilians-Universität (LMU) München, Munich, Germany. His current research interests include experiments on studying and applying entanglement, e.g., in various demonstrations of quantum communication protocols, in free-space quantum cryptography over record distances of 144 km, or in atom-photon entanglement.