# OSA® Publishing

# Handheld free space quantum key distribution with dynamic motion compensation

Hyunchae Chun, Iris Choi, Grahame Faulkner, Larry Clarke, Bryan Barber, Glenn George, Colin Capon, Antti Niskanen, Joachim Wabnig, Dominic O'Brien, and David Bitauld

✉  ⋖

“„ ▾  📄 **(viewmedia.cfm?uri=oe-25-6-6784&seq=0)**  ⦅!⦆

📑 **(/user/favorites_add_article.cfm?articles=361628)**

🔓 **Accessible**
Open Access

| Article Text | ⌄ |
|---|---|

| Figures (5) |
|---|

| Equations (5) |
|---|

| References (29) |
|---|

| Cited By (0) |
|---|

| Metrics |
|---|

| Back to Top |
|---|

🗎 **Get PDF (viewmedia.cfm?uri=oe-25-6-6784&seq=0)**

# Abstract

Mobile devices have become an inseparable part of our everyday life. They are used to transmit an ever-increasing amount of sensitive health, financial and personal information. This exposes us to the growing scale and sophistication of cyber-attacks. Quantum Key Distribution (QKD) can provide unconditional and future-proof data security but implementing it for handheld mobile devices comes with specific challenges. To establish security, secret keys of sufficient length need to be transmitted during the time of a handheld transaction (~1s) despite device misalignment, ambient light and user's inevitable hand movements. Transmitters and receivers should ideally be compact and low-cost, while avoiding security loopholes. Here we demonstrate the first QKD transmission from a handheld transmitter with a key-rate large enough to overcome finite key effects. Using dynamic beam-steering, reference-frame-independent encoding and fast indistinguishable pulse generation, we obtain a secret key rate above 30kb/s over a distance of 0.5m.

# 1. Introduction

Guaranteed by the laws of physics, Quantum Key Distribution (QKD) provides an ultimate level of security [1–3], and uniquely it is the only technology known to-date that can monitor eavesdropping activities. Since its inception in 1984, developments of QKD has been largely focused on securing large-scale infrastructures [4–6] using long distance fiber transmission [7–11] and free space transmission between fixed terminals [12–14] QKD transmission has also been demonstrated from large mobile vehicles such as trucks [15], planes [16] and air balloons [17]. Today, there is increasing demand for security in handheld devices such as mobile phones and wearable technologies. A QKD protected link between handheld devices and the terminal would provide the keys for encryption with verifiable security for any wireless communication system, ranging from indoor wireless networks (e.g. Wi-Fi) to access control and near field communications (NFC) mobile payment applications. This technology could also prevent ATM skimming attacks, where a $2 billion loss worldwide in 2015 [18] was estimated, by transmitting the quantum encryption key from the mobile device securely to the ATM terminal. A short-range free-space implementation of QKD could address these security challenges and provide a high degree of security.

For a handheld free-space QKD to be practical, it needs to be compact and low-cost [19–21], and crucially, it must also be able to transmit a secure key in a time suitable for a handheld transaction (~1s). If the size of the transmitted key is too small it is not mathematically secure, so during this short span of time, a number of qubits large enough to overcome finite key effects must be exchanged [22–24]. The system must therefore provide a stable communication link taking into account the user's unavoidable hand movement, which lead to translations and rotations of the mobile device. Previous work by Mélen, G. et al. [21] obtained intermittent key transmission from a handheld device by using one-side beam-steering and mechanical waveplate rotation in the receiver. Here we addressed these issues by using novel agile dual-MEMS mirror-based beam-steering system combined with a reference frame independent (RFI) QKD

protocol to provide wider angular, translational tolerance and rotational independence respectively. This results in the first stable quantum link from a handheld device able to transmit a secure key in less than a second.

In order to compensate for hand-held operation instabilities, we characterized typical hand-movement and accordingly designed a system with optimal latency and tolerance. Based on this evaluation, we implemented the system using MEMs mirrors for beam-steering at both ends of the link. Their orientation was controlled by a tracking system using LED beacons and Position sensing detectors (PSD) at both ends of the steering system. This implementation allowed us to obtain a wide angular coverage and minimize latency, thus guaranteeing the robustness against hand movements.

The RFI QKD protocol proposed by Laing, A. et al. [25], and experimentally demonstrated by Wabnig, J. et al. [26] allows polarization encoding without the requirement of aligning the polarization bases. In this protocol the qubits are encoded and measured in three polarization bases (horizontal-vertical, diagonal-anti-diagonal, circular left-circular right). Only one of those bases needs to have a fixed alignment between the transmitter and the receiver. As the circular basis is unaffected by relative rotations of the transmitter and the receiver in polarization encoding, it is therefore used to transmit the secret keys. The two linear bases can have any relative alignment and are used to assess the security parameters of the quantum channel. Based on this protocol, we demonstrated a practical quantum secured wireless link between a terminal and a handheld device using a steerable optical link.

# 2. System design

## 2.1 QKD transmitter and receiver modules

The RFI QKD transmitter and receiver modules are represented in **Figs. 1(a) and 1(b)** respectively. RFI QKD is based on the transmission and detection of qubits encoded in three bases. Here the qubits are implemented by polarization encoded faint pulses. In order to produce these 6 optical states, we use 6 resonant-cavity Light Emitting Diodes (RCLEDs). The light produced by each of the RCLED is collimated and transmitted through a set of Polarizing Beam Splitters (PBS), non-polarizing Beam Splitters (BS) and waveplates (WP). The polarization of the light produced by each RCLED is thus purified and rotated in order to exit the transmitter in one of the 6 required polarization states. The optical signal is then attenuated by a neutral density (ND) filter to obtain faint pulses.
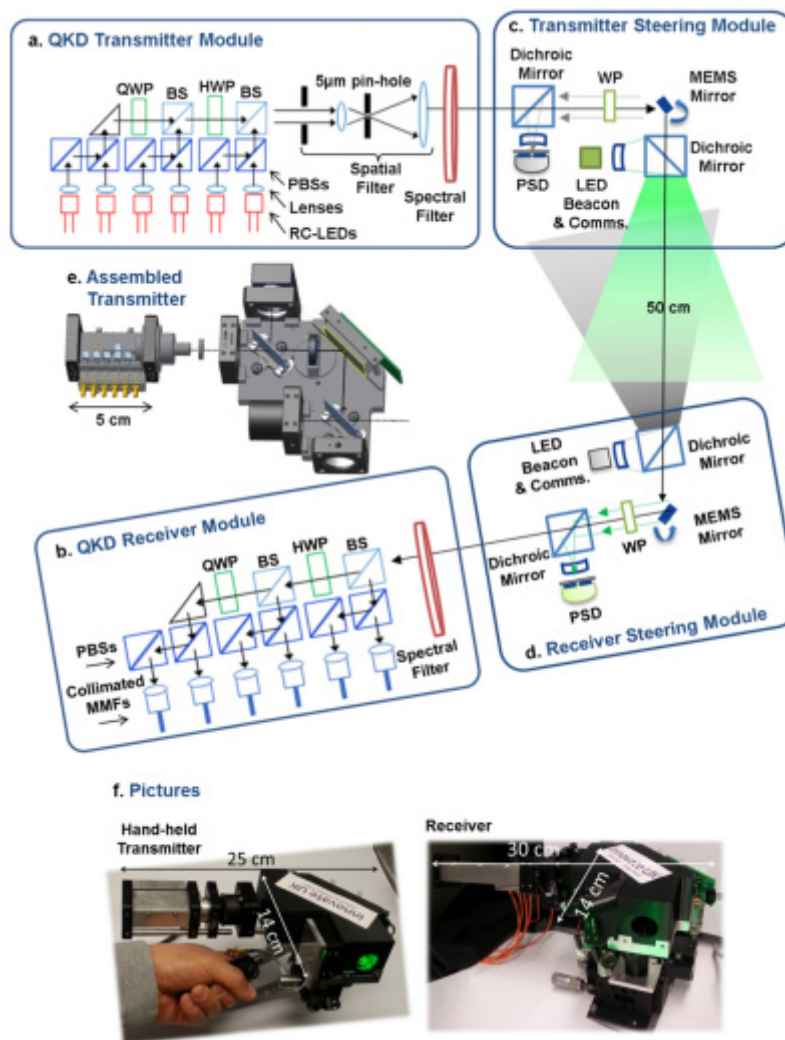
**Fig. 1** Hand-held QKD device and terminal. (a), (b) RFI protocol based QKD transmitter and receiver module. (c), (d) A schematic representation of beam-steering modules with50cm optical link. (e) Assembled transmitter showing the QKD and steering module. (f) Experimenter holding the hand-held transmitter, also showing the receiver module in use.
Download Full Size (/viewmedia.cfm?uri=oe-25-6-6784&figure=oe-25-6-6784-g001&imagetype=full) | PPT Slide (/viewmedia.cfm?uri=oe-25-6-6784&figure=oe-25-6-6784-g001&imagetype=pwr) | PDF (/viewmedia.cfm?uri=oe-25-6-6784&figure=oe-25-6-6784-g001&imagetype=pdf)

In order to avoid side-channel attacks [27] the optical states originating from all the RCLEDs must be identical apart from their polarizations. This means that their spatial, spectral, and time profiles should be identical. For the spatial indistinguishability, a spatial filter composed of a first aperture with a 1mm diameter followed by a focusing lens (f = 6.24mm) and a second aperture with a 5 micron diameter (comparable to the Airy disk diameter). The light is then collimated with an f = 11mm lens. This ensures any difference in mode profile or propagation direction between sources is eliminated. In order to ensure the spectral indistinguishability, a spectral filter with a passband (1.5 nm centred at 658 nm) narrower than the RCLED emission spectrum (spectral width of 7nm, central wavelength of ~656 nm) is used to select the light to be transmitted. **Figure 2(a)** shows the resulting spectra from the six sources. Here, the choice of RCLEDs over laser diodes or LEDs is important since RCLEDs have a wider spectrum than lasers, without multiple

mode structure. The disparities between the central wavelengths of the different RC-LEDs become smaller as the light going through a narrow band filter will be similar for each RC-LED (**Fig. 2(a)**). This is very difficult to achieve with lasers because they need to be tuned with a tolerance smaller than their individual modes' width and filtered with a narrower filter. Since RCLEDs can be modulated faster than LEDs, it is possible to transmit a larger number of photons compared to the constant detector noise rate and thus, increasing the key rate. Time profiles of the light emitted by each source were measured by a single photon detector collecting photons at the output of the transmitter. The resulting statistics, shown on **Fig. 2(b)**, exhibits a very good timing overlap. To modularize both the transmitter and receiver, base plates were fabricated using aluminum terminated with modified 16mm cage plates to house the spatial filter and to enable easy integration with the beam-steering system. Alignment of the receiver's lensed multimode fibers was achieved using spherical bearings to give the degrees of freedom required. All components were fixed in place using UV cured adhesives. In the demonstration the RCLEDs were driven by a 6-channel pattern generator. Every 4ns (i.e. a 250MHz repetition rate), a 1ns pulse is generated in one of the six channels, this channel being determined by a pseudo-random pattern. The voltage level driving each channel is adjusted to ensure that the output power was identical for the 6 polarizations. The power was then reduced to 0.07 photons per pulse with a ND filter (10dB). This value was chosen to obtain a sufficiently small probability for a pulse to contain more than one photon.
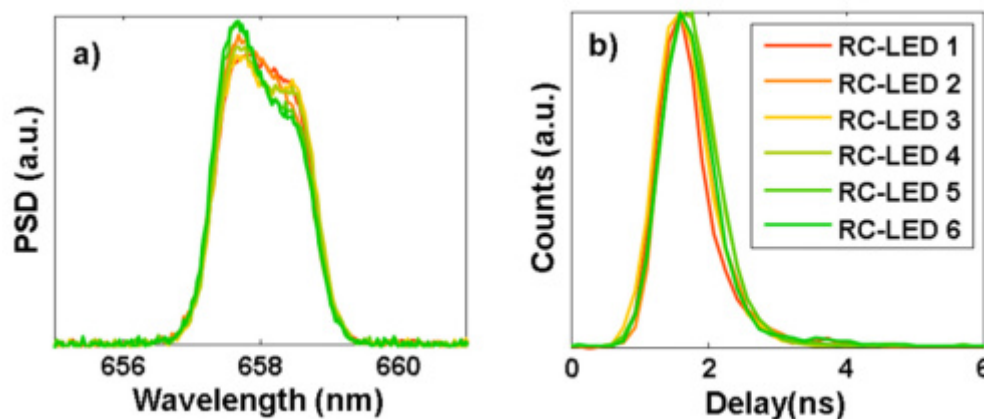


**Fig. 2** RC LED characteristics. (a) Optical spectrum of the light generated by each RC-LED after going through the spectral filter. (b) Arrival time statistics for photons generated by each RC-LED. The x-axis is the delay with respect to the synchronization signal.
Download Full Size (/viewmedia.cfm?uri=oe-25-6-6784&figure=oe-25-6-6784-g002&imagetype=full) | PPT Slide (/viewmedia.cfm?uri=oe-25-6-6784&figure=oe-25-6-6784-g002&imagetype=pwr) | PDF (/viewmedia.cfm?uri=oe-25-6-6784&figure=oe-25-6-6784-g002&imagetype=pdf)

The receiver module (**Fig. 1(b)**) has a similar structure to the transmitter. First, the light is spectrally filtered with the same passband as the transmitter filter. Then, light propagates through the same PBS, BS and WP arrangement as the transmitter, which splits the light according to its polarization and distributes it to six different channels. Light is then coupled into six lensed multimode fibers, which are connected to the

Silicon Avalanche Photo-Detectors (SiAPD). The resulting photon counts are used to assess the security parameters of the quantum channel and build a secret key. Based on this protocol, we demonstrated a practical quantum secured wireless link.

## 2.2 Beam-steering module

The beam-steering module must compensate for hand movement, and ensure that the angular misalignment of the transmitter and receiver remains within the field of view of the QKD communications system. The angular fluctuations of typical hand movements were analyzed by measuring the position of a hand-held laser pointer spot as a function of time. **Figure 3(a)** shows the complementary cumulative distribution function (CCDF) of the angle created by hand-movement. This indicates the speed at which any correction must be made to the field of view of the optical system. Our receiver's the field of view, which is set by the numerical aperture of the lensed multimode fibers and associated optics, is 0.1 degree. This means that corrections must be made within approximately 42ms.
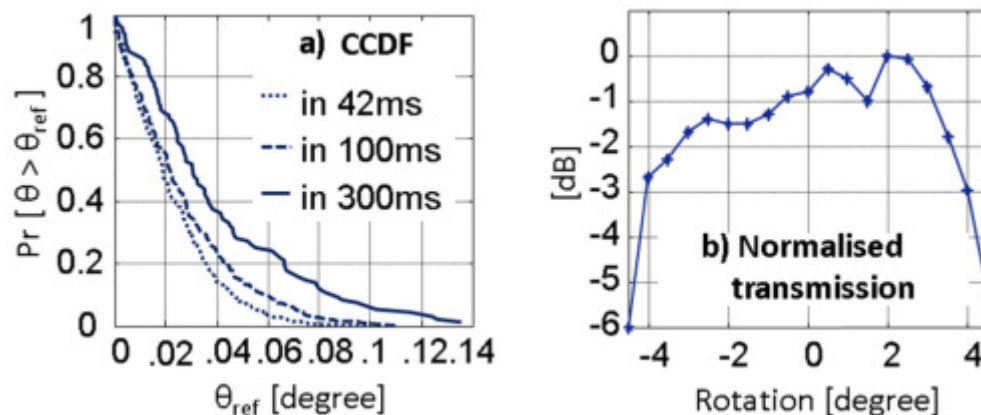


**Fig. 3** Hand-movement statistics and beam-steering coverage. (a) Complementary cumulative distribution function (CCDF) of the maximum angle deviation created by hand-movement in different time durations of 42ms, 100ms, and 300ms, where $\theta_{ref}$ is reference angle used for the CCDF (b) Normalized transmission loss by beam-steering with respect to the rotation of transmitter angle.
Download Full Size (/viewmedia.cfm?uri=oe-25-6-6784&figure=oe-25-6-6784-g003&imagetype=full) | PPT Slide (/viewmedia.cfm?uri=oe-25-6-6784&figure=oe-25-6-6784-g003&imagetype=pwr) | PDF (/viewmedia.cfm?uri=oe-25-6-6784&figure=oe-25-6-6784-g003&imagetype=pdf)

To minimize the system latency, a scheme using independent LED beacons is used here. Each terminal has a beacon that indicates its position, and a position sensitive detector (PSD) to measure the location of the beacon on the other terminal. This dual beacon system allows the two terminals to track each other independently, resulting in low-latency. **Figure 1(c), (d)** shows the system we used for dynamic beam-steering. A green LED beacon aligned with the QKD optical mode is used in the transmitter, to indicate its position to the receiver, allowing it to perform adjustment of its field of view. For the receiver to evaluate the transmitter's position, light from the beacon enters the receiver and is diverted to a PSD via a MEMs

steering mirror. The PSD then measures the angle of arrival of the beacon light, creating a signal that steers the MEMs mirror until the beacon light is centered on the PSD. This sets the receiver mirror angles so that photons coming from the direction of the QKD transmitter are coupled into the lensed fibers. The receiver also has a co-aligned infrared LED beacon, which allows the transmitter to orientate its MEMs mirror and steer the QKD photons towards the receiver. For this operation, beacon wavelengths (520nm for downlink, 850nm for uplink) were chosen to ensure enough separations from the weak QKD signal at 658nm via dichroic beam splitters. Commercial PSDs and MEMS mirrors were used. Mirror size ($\phi$ = 4.2mm) was chosen considering the fact that larger size leads to longer latency, mainly due to the inertia, but provides a better reliability by reflecting more off-axis beams. This PSD and MEMS mirror combination enabled a low latency suitable for an agile correction of hand-movement. In operation, coverage of +/−4 degree was achieved, as shown in **Fig. 3(b)**. For different link distances, divergence of the beacon lights (i.e., coverage) should be readjusted, so that the two PSDs can detect the light levels within their dynamic-range.

In addition, a waveplate was added in each steering module to correct for their induced birefringences. The WP angle around vertical axis as well as the relative angle of the QKD and steering modules were adjusted to obtain perfectly circular polarizations in the Z basis. We also took advantage of the fact that the additional WP acted essentially as a quarter WP to swap the X and Z basis by rotating the QKD receiver module by 45 degree. This allows us to have the Z basis (used for the secure key) nearer to the receiver input. By construction this made the detection probability and the polarization purity higher than when the Z basis is at the opposite end of the receiver.

# 3. QKD performance evaluation

In our QKD protocol part of the detected photons is used to build a raw key and the other part is used to estimate channel security parameters. The raw key is built by randomly extracting half of the photons that were transmitted as well as received in the Z basis. The remaining photon detections are used for security parameter estimation. In order to ensure absolute secrecy of the transmitted key, the raw key needs to be processed using error correction and privacy amplification codes. These reduce the key size to a fraction of its original size, called the secure key fraction. This secure key fraction is calculated based on the estimated security parameters, which are correlations between the number of photons transmitted in each polarization state and the number of detections in each receiver channel, using the method based on Wabnig, J. et al. [26]. These calculations take into account potential polarization impurity and non-orthogonality and it includes finite key analysis. Initial static tests were undertaken, for different steering angles. It was found that the optical elements in the beam-steering system (and to a small extent the beam splitters inside the transmitter and the receiver) introduced an undesired birefringence leading to polarization rotations of the QKD beams. RFI QKD is tolerant to polarization rotations, but not to ellipticity alterations, so a WP was added inside the beam-steering modules to compensate for this. The induced birefringence was also dependent on the MEMS mirror angle, which varies, and therefore cannot be compensated with a static WP, but it was found that the increase in the error rate remained within 3% over the whole steering range.

In order to demonstrate the robustness of our system against axial rotations (i.e. rotations around the transmission direction) we introduced a rotating half-wave plate between the emitter and the receiver, which is equivalent to a rotation of the transmitter by an angle equal to twice the value of the waveplate angle. The secure key fraction as a function of the equivalent rotation angle is shown on **Fig. 4**. Here the secure key fraction was calculated for 0.5s key transmissions. We can see that not only transmission of secure keys was possible for any angle but the secure key fraction remained between 40% and 60% over a 360 degree rotation. The secure key fraction was also calculated by using the BB84 protocol with the same photon counts, and therefore keeping two bases out of three to calculate the key fraction. In this case we can see that the system performances would drop very quickly with the transmitter angle. RFI protocols is superior to BB84 for each point except for the angle of 170 degrees. This is due to the fact that the calculation we used for the BB84 curves assumes perfect polarization orthogonality, while our RFI calculation takes the most pessimistic possibility without assuming perfect polarization. Rotations around the other axes induced small modifications of the photons' polarization but with minor effects on the secure key fraction. The secure key fraction over the whole possible range of deflection of the mirrors remained between 35% and 65%.
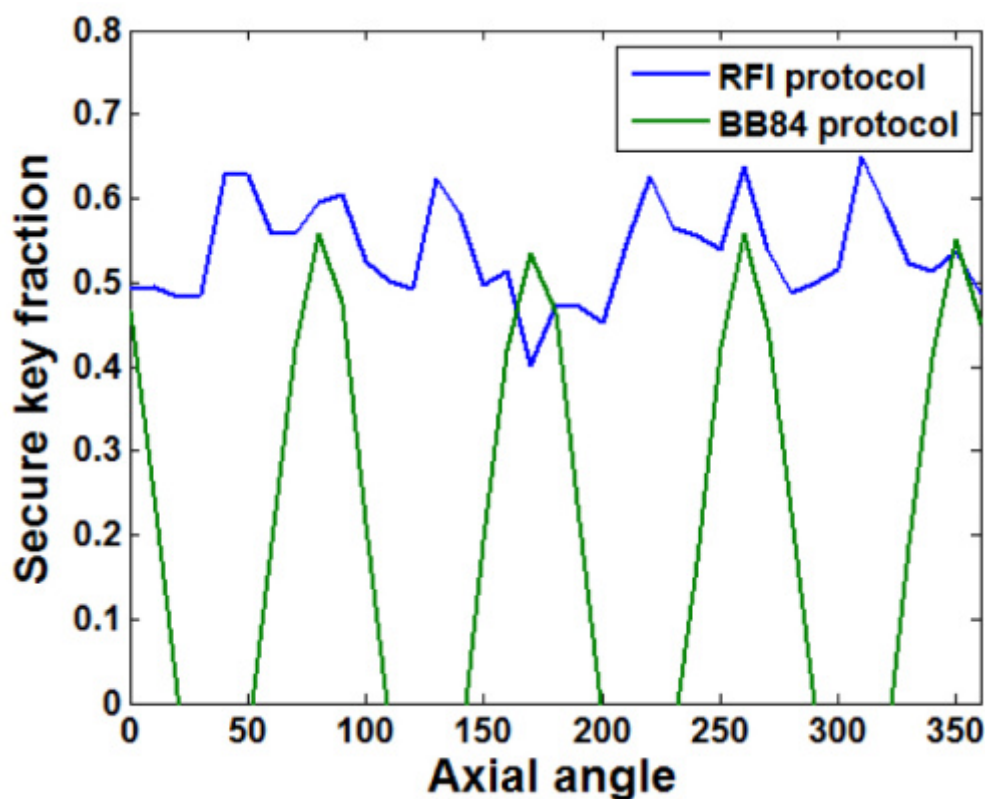


Fig. 4 Robustness of RFI protocol against axial rotation. The secure key fraction (ratio between the raw key length and the error corrected, privacy amplified key length) is plotted as a function of the relative axial angle between the transmitter and the receiver. The values were calculated from a 0.5s data transmission for each point, for a fixed position of the terminals. The relative axial angle between the transmitter and the receiver was simulated by rotating a half-wave plate between the terminals.

The system operates in normal ambient light conditions (>400 lux from incandescent light bulbs). The detector dark count rate is 370 counts/s per detector, and the noise due to ambient light was 600 photons/s per detector. The beacon LEDs additionally contribute approximately 570 photons/s per detector. These numbers are small compared to the ~1M photons/s that are detected for the QKD link, and induced error rate due to these impairments is negligible.

Quantum Key Distribution from a handheld device was demonstrated by holding the transmitter and pointing it at a static receiver. The whole optical assembly including the QKD and beam steering modules were part of the mobile handheld device, while the electrical instruments were static and connected to the handheld part by cables. Two sets of experiments were performed.

First, in order to illustrate the fluctuations of the asymptotic key rate in real time, measurements were performed while the experimenter holding the device performed a series of voluntary movements. To calculate this asymptotic key rate, short (4ms) samples of QKD transmission were collected every 100ms, which is the time required to process the photon arrival times.

**Figure 5(a)** shows the vertical and horizontal angles of the two MEMS mirrors as well as the axial angle. Mirror angles were derived from the applied voltage while the axial angle was derived from the photon statistics, which depend on the polarization angle. The alignment system was switched on after 4s, and no data was received before this point. Then we can see that the experimenter moves the transmitter up, down, left, right and finally performs an axial rotation. **Figure 5(b)** shows the transmission and error rate as a function of time. The transmission is defined as the total number of detected photons divided by the total number of emitted photons (i.e. 0.07 x 250MHz), while the error rate only takes into account the photons used for the secure key (i.e. photons transmitted and received in the Z basis). After starting the steering system, the transmission stabilizes at around 6% with a few short drops and the error rate is also approximately 6%. **Figure 5(c)** shows an estimation of the asymptotic key rate as a function of time, indicating a rate of approximately 30kb/s with very few drops to zero. Fluctuations in this rate are due to the short measurement samples.
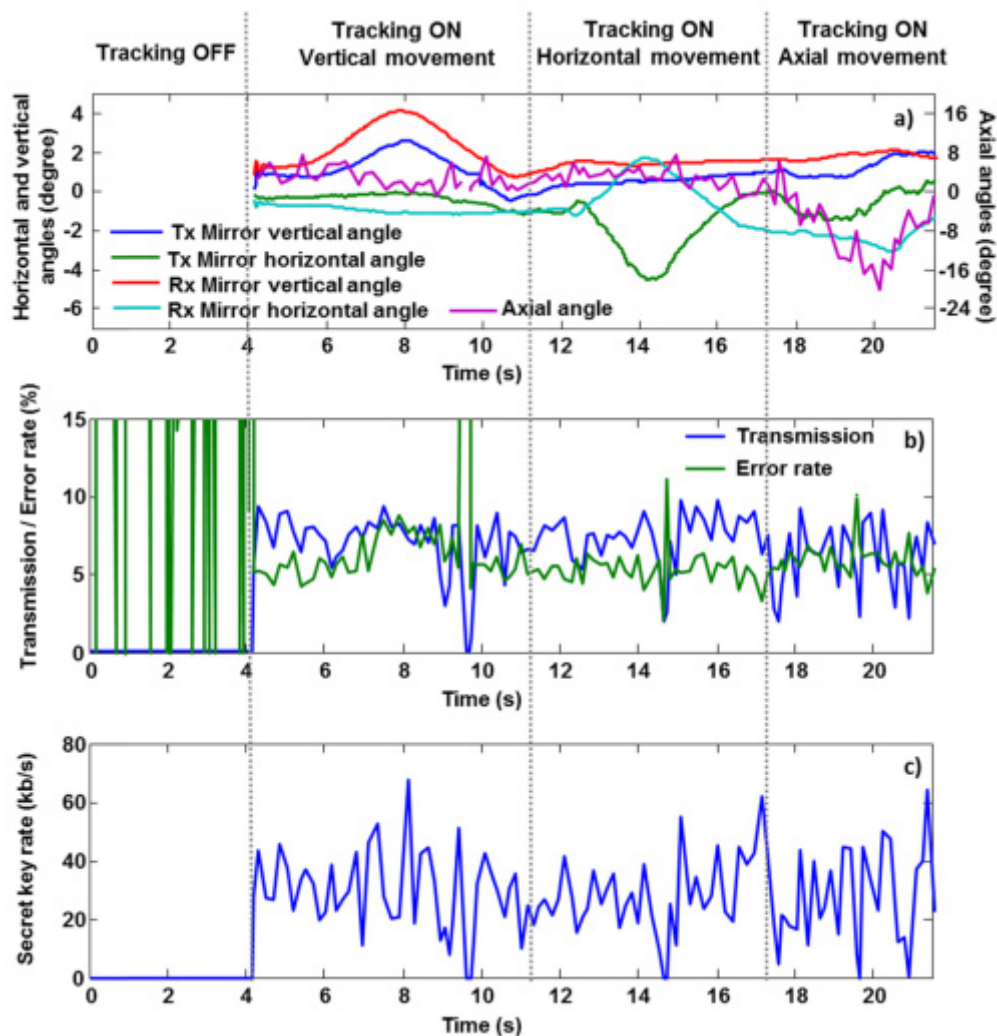
**Fig. 5** Hand-held QKD performance. These measurements were performed while the experimenter holding the QKD transmitter displaces it in the directions shown. The motion compensation system was switched on after 4s. (a)Vertical and horizontal angles of the two MEMS mirrors as well as the axial angle between the two terminals. The mirror angles were retrieved from the applied voltage, while the axial angle was calculated from the QKD data. This angle was divided by four to allow a common axis. (b) Photon transmission and error rate. The transmission is defined as the number of detected photons divided by the number of emitted photons (i.e. 0.07 x 250MHz). The error rate is calculated for photons that were both transmitted and detected in the Z basis. (c) Estimation of the asymptotic key rate as a function of time. Each point was calculated from a 4ms transmission sample.

Download Full Size (/viewmedia.cfm?uri=oe-25-6-6784&figure=oe-25-6-6784-g005&imagetype=full) | PPT Slide (/viewmedia.cfm?uri=oe-25-6-6784&figure=oe-25-6-6784-g005&imagetype=pwr) | PDF (/viewmedia.cfm?uri=oe-25-6-6784&figure=oe-25-6-6784-g005&imagetype=pdf)

Second, in order to demonstrate the performance of our system during a real handheld transaction, including the finite key effects, a series of 14 separate measurements was performed with a duration of 0.5s each, while the experimenter was holding the transmitter without any intentional movement. The average value of the secure key rate, after the finite key effect is taken into account, was 39kb/s with a

standard deviation of 8kb/s. These results show that our system can reliably transmit secret keys long enough to overcome the finite key limitations in a very short time. An increased key rate could be achieved by using a decoy state protocol [28,29]. This would however require more pseudo-random pattern channels to modulate the pulse amplitude.

# 4. Conclusions

In this paper, we have successfully constructed the first quantum wireless prototype for handheld usage fulfilling finite key requirements. The beam-steering technique used maintained a motion-stabilized communication link, which allowed sufficient secure keys to be transmitted with a high throughput under hand-movement and typical ambient light levels. A number of improvements are possible, for example, decoy state protocol could be implemented to increase the key rate. For full mobile device integration, further miniaturization of the emitter could be obtained by fabricating the RCLEDs on a single chip and combining the polarizations with photonic waveguides as previously demonstrated with VCSELs [20]. The steering system could also be miniaturized by taking advantage of the fast improvements and size reductions of laser-based pico-projection systems.

The success of wireless QKD technology could introduce an unprecedented level of data security to merchants and customers alike. Making QKD economical and practical enough is essential to overcome the adoption barrier before security threats start to appear with the increase of computing power and efficiency of hacking techniques. This demonstration of handheld quantum wireless prototype represents a major step towards real-world quantum security for mobile applications.

# 5 Appendix

## 5.1 QKD secure key rate calculations

Our security analysis takes into account that, in real implementations, not only reference frames of the transmitter and the receiver can be rotated with respect to each other, but also that there is always a degree of misalignment within a reference frame. This induces non-orthogonality within a basis and mutual bias between bases. Our analysis also takes into account differing detector efficiencies. This is achieved by using an explicit device model and minimizing the key rate over possible model parameters. 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.

Following the derivation in Wabnig, J. et al. [26], we can express the secret key fraction as

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

We take into account imperfect measurement devices that 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 $\alpha$. The usable entropy is obtained as the minimum over

all parameters $\alpha$, $\lambda_{1,2}$

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

The parameters have to obey the constraints imposed by the observations

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, 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 consisting of 9 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 $f_i$ . To obtain the secret key fraction we need to subtract the observed relative entropy in the key bases from the usable entropy

The full set of measurements enables us to calculate a reference frame independent key rate. From the detector counts we can construct 9 correlation functions

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

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.

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 angle), resulting in a total of 20 free parameters. Different absorption may occur in the preparation channels, and similarly detectors may have different efficiencies. With six possible preparation directions and six possible detection direction 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. 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. Finally, since we don't use single photon sources in the transmitter, we need to consider the occasional transmission of multi-photon pulses, which could be exploited by an adversary able to non-destructively detect those pulses and extract one of the photons. We also need to consider that the adversary could reduce the losses on the remaining photon, for example by steering this photon in a more efficient way than our system does. However, some losses inside the receiver module are not accessible by the adversary. We consider that misalignment losses are accessible by the adversary but the losses due to the optical elements' transmission and detector efficiency cannot be eliminated. In our case the transmission subtracted from the inaccessible losses is $t_E$=20.1%. For each data point, we then calculate the proportion $r_{mp}$ of photons used to build the secret key that could have originated from multi-photon pulses. According to Poisson statistics, the probability for a pulse to contain 1 photon is approximately 0.07 and the probability to have more than one photon is approximately $0.07^2/2$. For a system transmission $t_A$ (fluctuating over time), the proportion of photons potentially coming from multi-photon pulses $r_{mp}$=0.07/2×$t_E$/$t_A$. For example, if the transmission $t_A$ is 6%, $r_{mp}$ is equal to 0.12. Privacy amplification needs to be applied accordingly, which reduces our key rate by the factor 1-$r_{mp}$.

## 5.2 Axial angle estimation

The correlators defined in the above section can also be used to estimate the relative axial angle between the QKD bases of the transmitter and the receiver. Several combinations of correlators can be used to calculate the angle. These calculations based on single photon counts are intrinsically noisy. In order to reduce this noise a median of the different possible ways to retrieve the angle W was calculated:

$$-a\tan2(C_{YX}, C_{YY}) - 135, \quad -a\tan2(C_{XY}, C_{YY}) - 135)$$

The 45 degree rotation is due to the rotation of the QKD module in the receiver. This calculation is based on the photon counts, and a low transmission does not allow us to retrieve an accurate angle. This is why there is a missing section in **Fig. 5(a)** in the manuscript around 9.5 seconds. This corresponds to a transmission drop.

# Funding

# References and links

**1.** C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution," in International Conference on Computer System and Signal Processing (IEEE, 1984), pp. 175–179.

**2.** A. K. Ekert, "Quantum cryptography based on Bell's theorem," Phys. Rev. Lett. **67**(6), 661–663 (1991). [**CrossRef** (http://dx.doi.org/10.1103/PhysRevLett.67.661)] ☑ [**PubMed** (http://www.ncbi.nlm.nih.gov/pubmed/10044956)] ☑

**3.** N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," Rev. Mod. Phys. **74**(1), 145–195 (2002). [**CrossRef (http://dx.doi.org/10.1103/RevModPhys.74.145)**] ⬀

**4.** D. Stucki, M. Legré, F. Buntschu, B. Clausen, N. Felber, N. Gisin, L. Henzen, P. Junod, G. Litzistorf, P. Monbaron, L. Monat, J.-B. Page, D. Perroud, G. Ribordy, A. Rochas, S. Robyr, J. Tavares, R. Thew, P. Trinkler, S. Ventura, R. Voirol, N. Walenta, and H. Zbinden, "Long-term performance of the SwissQuantum quantum key distribution network in a field environment," New J. Phys. **13**(12), 123001 (2011). [**CrossRef (http://dx.doi.org/10.1088/1367-2630/13/12/123001)**] ⬀

**5.** M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J. F. Dynes, A. R. Dixon, A. W. Sharpe, Z. L. Yuan, A. J. Shields, S. Uchikoga, M. Legré, S. Robyr, P. Trinkler, L. Monat, J. B. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Länger, M. Peev, and A. Zeilinger, "Field test of quantum key distribution in the Tokyo QKD Network," Opt. Express **19**(11), 10387–10409 (2011). [**CrossRef (http://dx.doi.org/10.1364/OE.19.010387)**] ⬀  [**PubMed (http://www.ncbi.nlm.nih.gov/pubmed/21643295)**] ⬀

**6.** A. Mirza and F. Petruccione, "Recent findings from the quantum network in Durban," AIP Conf. Proc. **1363** (2011), 35–38 (2011).

**7.** D. Stucki, N. Walenta, F. Vannel, R. T. Thew, N. Gisin, H. Zbinden, S. Gray, C. R. Towery, and S. Ten, "High rate, long-distance quantum key distribution over 250 km of ultra low loss fibers," New J. Phys. **11**(7), 075003 (2009). [**CrossRef (http://dx.doi.org/10.1088/1367-2630/11/7/075003)**] ⬀

**8.** C. Gobby, Z. L. Yuan, and A. J. Shields, "Quantum key distribution over 122 km of standard telecom fiber," Appl. Phys. Lett. **84**(19), 3762–3764 (2004). [**CrossRef (http://dx.doi.org/10.1063/1.1738173)**] ⬀

**9.** P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, "Experimental demonstration of long-distance continuous-variable quantum key distribution," Nat. Photonics **7**(5), 378–381 (2013). [**CrossRef (http://dx.doi.org/10.1038/nphoton.2013.63)**] ⬀

**10.** J. F. Dynes, I. Choi, A. W. Sharpe, A. R. Dixon, Z. L. Yuan, M. Fujiwara, M. Sasaki, and A. J. Shields, "Stability of high bit rate quantum key distribution on installed fiber," Opt. Express **20**(15), 16339–16347 (2012). [**CrossRef (http://dx.doi.org/10.1364/OE.20.016339)**] ⬀

**11.** J. F. Dynes, H. Takesue, Z. L. Yuan, A. W. Sharpe, K. Harada, T. Honjo, H. Kamada, O. Tadanaga, Y. Nishida, M. Asobe, and A. J. Shields, "Efficient entanglement distribution over 200 kilometers," Opt. Express **17**(14), 11440–11449 (2009). [**CrossRef (http://dx.doi.org/10.1364/OE.17.011440)**] ⬀ [**PubMed (http://www.ncbi.nlm.nih.gov/pubmed/19582059)**] ⬀

**12.** R. J. Hughes, J. E. Nordholt, D. Derkacs, and C. G. Peterson, "Practical free-space quantum key distribution over 10 km in daylight and at night," New J. Phys. **4**, 43 (2002). [**CrossRef (http://dx.doi.org/10.1088/1367-2630/4/1/343)**] ⬀

**13.** R. Alléaume, F. Treussart, G. Messin, Y. Dumeige, J. F. Roch, A. Beveratos, R. Brouri-Tualle, J. P. Poizat, and P. Grangier, "Experimental open-air quantum key distribution with a single-photon source," New J. Phys. **6**, 92 (2004). [**CrossRef (http://dx.doi.org/10.1088/1367-2630/6/1/092)**] ⬀

**14.** R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Ömer, M. Fürst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter, and A. Zeilinger, "Entanglement-based quantum communication over 144 km," Nat. Phys. **3**(7), 481–486 (2007). [**CrossRef (http://dx.doi.org/10.1038/nphys629)**] ⬀

**15.** J.-P. Bourgoin, B. L. Higgins, N. Gigov, C. Holloway, C. J. Pugh, S. Kaiser, M. Cranmer, and T. Jennewein, "Free-space quantum key distribution to a moving receiver," Opt. Express **23**(26), 33437–33447 (2015). [**CrossRef (http://dx.doi.org/10.1364/OE.23.033437)**] ⬀ [**PubMed (http://www.ncbi.nlm.nih.gov/pubmed/26832008)**] ⬀

**16.** S. Nauerth, F. Moll, M. Rau, C. Fuchs, J. Horwath, S. Frick, and H. Weinfurter, "Air-to-ground quantum communication," Nat. Photonics **7**(5), 382–386 (2013). [**CrossRef (http://dx.doi.org/10.1038/nphoton.2013.46)**] ⬀

**17.** J.-Y. Wang, B. Yang, S.-K. Liao, L. Zhang, Q. Shen, X.-F. Hu, J.-C. Wu, S.-J. Yang, H. Jiang, Y.-L. Tang, B. Zhong, H. Liang, W.-Y. Liu, Y.-H. Hu, Y.-M. Huang, B. Qi, J.-G. Ren, G.-S. Pan, J. Yin, J.-J. Jia, Y.-A. Chen, K. Chen, C.-Z. Peng, and J.-W. Pan, "Direct and full-scale experimental verifications towards ground-satellite quantum key distribution," Nat. Photonics **7**(5), 387–393 (2013). [**CrossRef (http://dx.doi.org/10.1038/nphoton.2013.89)**] ⬀

**18.** "Revised best practices guide counters ATM skimming scourge." [Online]. Available: **http://www.atmmarketplace.com/news/revised-best-practices-manual-counters-atm-skimming-scourge (http://www.atmmarketplace.com/news/revised-best-practices-manual-counters-atm-skimming-scourge)**.

**19.** J. L. Duligall, M. S. Godfrey, K. A. Harrison, W. J. Munro, and J. G. Rarity, "Low cost and compact quantum key distribution," New J. Phys. **8**(10), 249 (2006). [**CrossRef (http://dx.doi.org/10.1088/1367-2630/8/10/249)**] ⬀

**20.** G. Vest, M. Rau, L. Fuchs, G. Corrielli, H. Weier, S. Nauerth, A. Crespi, R. Osellame, and H. Weinfurter, "Design and evaluation of a handheld quantum key distribution sender module," IEEE J. Sel. Top. Quantum Electron. **21**(3), 131–137 (2015). [**CrossRef (http://dx.doi.org/10.1109/JSTQE.2014.2364131)**] ⬀

**21.** G. Mélen, T. Vogl, M. Rau, G. Corrielli, A. Crespi, R. Osellame, and H. Weinfurter, "Integrated quantum key distribution sender unit for daily-life implementations," Proc. SPIE **9762**, 97620A (2016). [**CrossRef (http://dx.doi.org/10.1117/12.2208643)**] ⬀

**22.** L. Sheridan, T. P. Le, and V. Scarani, "Finite-key security against coherent attacks in quantum key distribution," New J. Phys. **12**(12), 123019 (2010). [**CrossRef (http://dx.doi.org/10.1088/1367-2630/12/12/123019)**] ⬀

**23.** T. Meyer, H. Kampermann, M. Kleinmann, and D. Bruß, "Finite key analysis for symmetric attacks in quantum key distribution," Phys. Rev. A **74**(4), 042340 (2006). [**CrossRef (http://dx.doi.org/10.1103/PhysRevA.74.042340)**] 🔗

**24.** V. Scarani and R. Renner, "Quantum cryptography with finite resources: unconditional security bound for discrete-variable protocols with one-way postprocessing," Phys. Rev. Lett. **100**(20), 200501 (2008). [**CrossRef (http://dx.doi.org/10.1103/PhysRevLett.100.200501)**] 🔗 [**PubMed (http://www.ncbi.nlm.nih.gov/pubmed/18518517)**] 🔗

**25.** A. Laing, V. Scarani, J. G. Rarity, and J. L. O'Brien, "Reference-frame-independent quantum key distribution," Phys. Rev. A **82**(1), 012304 (2010). [**CrossRef (http://dx.doi.org/10.1103/PhysRevA.82.012304)**] 🔗

**26.** J. Wabnig, D. Bitauld, H. W. Li, A. Laing, J. L. O'brien, and A. O. Niskanen, "Demonstration of free-space reference frame independent quantum key distribution," New J. Phys. **15**(7), 073001 (2013). [**CrossRef (http://dx.doi.org/10.1088/1367-2630/15/7/073001)**] 🔗

**27.** S. Nauerth, M. Fürst, T. Schmitt-Manderbach, H. Weier, and H. Weinfurter, "Information leakage via side channels in freespace BB84 quantum cryptography," New J. Phys. **11**(6), 065001 (2009). [**CrossRef (http://dx.doi.org/10.1088/1367-2630/11/6/065001)**] 🔗

**28.** H.-K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," Phys. Rev. Lett. **94**(23), 230504 (2005). [**CrossRef (http://dx.doi.org/10.1103/PhysRevLett.94.230504)**] 🔗 [**PubMed (http://www.ncbi.nlm.nih.gov/pubmed/16090452)**] 🔗

**29.** W.-Y. Liang, S. Wang, H.-W. Li, Z.-Q. Yin, W. Chen, Y. Yao, J.-Z. Huang, G.-C. Guo, and Z.-F. Han, "Proof-of-principle experiment of reference-frame-independent quantum key distribution with phase coding," Sci. Rep. **4**, 3617 (2014). [**CrossRef (http://dx.doi.org/10.1038/srep03617)**] 🔗 [**PubMed (http://www.ncbi.nlm.nih.gov/pubmed/24402550)**] 🔗

# Optics Express

Andrew M. Weiner, Editor-in-Chief

**(/oe/home.cfm)**

About (/oe/journal/oe/about.cfm)

Issues in Progress (/oe/upcomingissue.cfm)

Current Issue (/oe/issue.cfm)

All Issues (/oe/browse.cfm)

Feature Issues (/oe/feature.cfm)

**Home (/)**                                                                                      **To Top ⬆**

◀ **Previous Article (abstract.cfm?uri=oe-25-6-6767)**         **Next Article** ▶ **(abstract.cfm?uri=oe-25-6-6796)**

**My Favorites** ▾

**Recent Pages** ▾

**Journals (/about.cfm)**

**Proceedings (/conferences.cfm)**

Information for

**Authors (/author/author.cfm)**

**Reviewers (/submit/review/peer_review.cfm)**

**Librarians (/library/)**

Other Resources

**OSAP Bookshelf (/books/default.cfm)**

**OIDA Reports (/oida/reports.cfm)**

**Optics & Photonics News** ⬀ **(http://www.osa-opn.org)**

**Optics ImageBank** ⬀ **(http://imagebank.osa.org)**

**Spotlight on Optics (/spotlight/)**

Regional Sites

**OSA Publishing China (/china/)**

About

**About OSA Publishing (/about.cfm)**

**About My Account (/benefitslog.cfm)**

**Contact Us (/contactus.cfm)**

**Send Us Feedback**