Article:

Modulator-Free Coherent-One-Way Quantum Key Distribution

G. L. Roberts, M. Lucamarini, J. F. Dynes, S. J. Savory, Z. L. Yuan,* and A. J. Shields

Time-bin encoding is an attractive method for transmitting photonic qubits over long distances with minimal decoherence. It allows a simple receiver for quantum key distribution (QKD) that extracts a key by measuring time of arrival of photons and detects eavesdropping by measuring interference of pulses in different time bins. In the past, coherent pulses have been generated using a CW laser and an intensity modulator. A greatly simplified transmitter is proposed and demonstrated here that works by directly modulating the laser diode. Coherence between pulses is maintained by a weak seed laser. The modulator-free source creates time-bin encoded pulses with a high extinction ratio (29.4 dB) and an interference visibility above 97 %. The resulting QKD transmitter gives estimated secure key rates up to 4.57 Mbit/s, the highest yet reported for coherent-one-way QKD, and can be programmed for all protocols using weak coherent pulses.

Quantum key distribution (QKD) uniquely allows two parties to exchange secure keys with secrecy guaranteed by the fundamental laws of physics.[1] Its potential for real-world applications has stimulated a large amount of progress in developing implementation technologies.[2] Over optical fiber links, QKD has been demonstrated to distribute quantum keys with rates exceeding 1 Mbit/s,[3] over a hundred kilometers of distance[4,5] and/or in the presence of strong classical signals in the same fiber.[6] The technology is being extensively tested in installed fiber network environments.[7] Moreover, satellite QKD and quantum repeater technologies are also being pursued to extend communication to the global scale.[2]

Since the inception of QKD in 1984 with the Bennett-Brassard (BB84) protocol,[8] a number of diverse implementations have been proposed. Two broad classes of protocol that share

G. L. Roberts, M. Lucamarini, J. F. Dynes, Z. L. Yuan, A. J. Shields
Toshiba Research Europe Limited
208 Cambridge Science Park, Milton Road, Cambridge, CB4 0GZ, United Kingdom
E-mail: zhiliang.yuan@crl.toshiba.co.uk
G. L. Roberts, S. J. Savory
Cambridge University Engineering Department
9 J J Thomson Avenue, Cambridge, CB3 0FA, United Kingdom

The ORCID identification number(s) for the author(s) of this article can be found under https://doi.org/10.1002/lpor.201700067

popularity are discrete variable and distributed phase reference protocols.[9] The protocols within these classes have a variety of requirements for transmitters, for example phase modulation and/or intensity modulation. Each provides different benefits, whether it is high bit rate, long achievable distance, a rigorous security proof or simplicity in experimental implementation. It is therefore highly beneficial to develop a versatile QKD transmitter that can operate different QKD protocols. Promising work has recently been demonstrated by combining a laser with a number of external phase and intensity modulating elements.[10]

The modulator-free transmitter proposed by Yuan *et al*[11] has a number of attractive properties for phase modulation. The light source uses a pair of laser diodes in an optical injection configuration. A master laser provides phase modulation, and randomization when required, while the slave laser is responsible for generating short optical pulses. The light source has successfully been demonstrated for two important phase-encoded QKD protocols, BB84 and differential phase shift (DPS).[12] However, the suitability of a modulator-free design to offer high extinction ratio intensity modulation in quantum communications is yet to be explored.

Here, we tackle this issue by implementing the coherent-one-way (COW) QKD protocol with a modulator-free transmitter. This transmitter allows us to achieve record-breaking key rates with quantum bit error rates (QBERs) below 1 % and visibilities over 97 %. Using a realistic finite key-size scenario, we can distribute keys from Alice to Bob at losses between 1.5 dB and 30 dB, equivalent to 7.5 km and 150 km of standard single mode optical fiber.

The COW protocol[4] uses time-bin encoding to share a key between two parties. Security of the key is ensured by Alice maintaining a fixed coherence between pulses. Bob can measure the interference visibility between adjacent pulses using an interferometer and infer the presence of an eavesdropper, Eve, by a break in the coherence. It has been used in a real-fiber system to transmit a secure key between two parties separated by 307 km - the longest distance for any two party quantum protocol.[4] This is possible because the time-bin encoding produces a lower QBER than other protocols, for example BB84.[3] The main downside to the protocol is that whilst security against a number of attacks has been demonstrated, no comprehensive security proof exists for all families of attack,[9] which could mean the protocol is vulnerable to an all-powerful Eve.
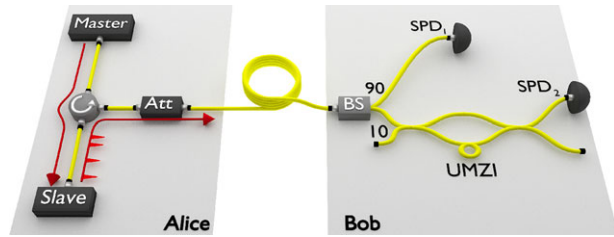
Figure 1. System schematics. The master laser in Alice injects CW light into the slave laser, which produces low-jitter gain-switched pulses. These are then attenuated to the single photon level before being transmitted through the quantum channel to Bob. SPD$_1$ detects the arrival time of the photons, from which the key is generated, and SPD$_2$ is used to measure the phase coherence. BS=beamsplitter; UMZI=unbalanced Mach-Zehnder interferometer; Att=attenuator.

In the COW protocol, Alice prepares two values of a logical bit using empty or full time bins: $|\beta_0\rangle = |\alpha\rangle|0\rangle$ and $|\beta_1\rangle = |0\rangle|\alpha\rangle$, where $|0\rangle$ is the vacuum state and $|\alpha\rangle$ represents a coherent state of light[13] with intensity $\mu = |\alpha|^2$. For these requirements, the transmitter used in this protocol must be able to modulate intensity whilst maintaining coherence. Bob decodes the signals by measuring their arrival times with a single photon detector (SPD). He also takes a portion of the received photons in order to measure the coherence between adjacent time bins, allowing him to test the channel against unauthorized external intrusions. This measurement is performed by overlapping two consecutive optical pulses on a beam splitter and measuring the resultant interference visibility. This is possible for the pulse sequence $|\beta_1\rangle|\beta_0\rangle$. To increase the number of consecutive non-empty pulses, Alice also prepares a decoy sequence $|\beta_2\rangle = |\alpha\rangle|\alpha\rangle$. This reduces the amount of bits Bob needs to collect before he can accurately measure the visibility, which is important in the finite key-size scenario. Moreover, the decoy sequence is used as a security feature, as Eve does not know whether she is attacking a logical bit or a decoy sequence. During sifting, Alice informs Bob when she sent decoy pulses and Bob tells Alice whether he measured the arrival time or the visibility of the optical pulses.

Figure 1 shows the experimental setup. The quantum transmitter (Alice) is configured for time-bin encoding using a slave laser that is optically seeded by a master laser. An optical attenuator attenuates the non-empty time bins to around 0.1 photons per pulse before transmitting them through the quantum channel, implemented by an optical attenuator, to the quantum receiver (Bob). Bob uses a 90:10 beamsplitter to passively route most of the photons to a superconducting nanowire detector (SPD$_1$) for arrival time measurements. The remaining 10 % are fed into an unbalanced Mach-Zehnder interferometer (UMZI) for measuring the phase coherence with a second superconducting nanowire detector (SPD$_2$). The UMZI is based on a planar lightwave circuit with a differential delay of 500 ps and has a loss of 3 dB. A built-in heater allows direct control of the phase delay across one arm. The superconducting nanowire SPDs used feature a dark count rate (DCR) of 10 Hz, alongside an efficiency of 34 % at a wavelength of 1550 nm, allowing us to reach long distances.

Intensity-modulated gain-switched pulses are produced through electrical modulation of the slave laser at 3.3 V.[14,15]

A DC bias above the lasing threshold is applied to the master laser to ensure the phase is coherent when it is injected into the slave laser. We use a wavelength-tunable, continuous-wave fiber laser as the master laser and a semiconductor distributed feedback (DFB) laser diode as the slave. The slave laser is kept at room temperature with a free-running wavelength of 1550.1 nm. The master laser is wavelength-tuned to give a maximum coherence transfer, which occurs when both lasers have the same free-running wavelength. The output pulses from this system have a pulse width of 70 ps, which is much smaller than the inverse modulation frequency, and a spectral width of 0.10 nm. For time-bin encoding, a pseudo-random number generator creates a repeated 512-bit sequence, generating decoy sequences with a probability of 1 % and signal sequences for the remaining time bins equally distributed between the bit values 0 and 1. The pattern generated is applied to gain-switch the slave laser at a clock rate of 2 GHz, therefore implementing a COW transmitter at an effective bit-rate of 1 GHz. A high intensity extinction ratio of 29.4 dB can be achieved between non-empty and empty pulses, thus ensuring a low encoding error in the time basis.

Optical injection ensures there is coherence among the gain-switched slave pulses, as they all inherit the phase of the CW master laser. The injected light transfers the coherence, thereby suppressing the randomness of the phase that would occur if pulses were triggered by spontaneous emission.[16] To illustrate the physical principle, we gain-switch the slave laser to produce a 2 GHz pulse train and replace the SPD$_2$ in Figure 1 with an optical power meter to measure the interference fringe visibility, defined as

$$V = \frac{I_{max} - I_{min}}{I_{max} + I_{min}}, \tag{1}$$

where I_{max} and I_{min} are the average pulse intensities for constructive and destructive interference respectively. The attenuator in Figure 1 is set to maximum transmission, while a second attenuator (not shown) is used to vary the seed optical power into the slave laser. The interference visibility increases monotonically with seed power, as a result of the increasing dominance of the injected light over spontaneous emission in the slave laser cavity. The visibility saturates at 99.78 % with a seed power of 216 μW. In order to achieve a visibility of 99 %, a modest 12 μW of seed power is sufficient. In the subsequent QKD experiment, we use a seed power of 50 μW to ensure the pulses are sub-100 ps.

The quantum transmitter and receiver are linked via a short optical fiber and extra attenuation is applied to simulate the loss of the quantum channel. The transmitting photon flux is set to 0.1 photons per non-empty pulse at the output of the transmitter. At the lowest attenuation we decrease the photon flux to 0.07 photons per pulse to minimize time-jitter effects, as described later. In the QKD experiment, two channels of a digitizer with 100 ps time resolution simultaneously record the arrival times of single photons at the photon detectors (SPD$_1$ and SPD$_2$). Bob uses a 90:10 beamsplitter to passively direct most of the photons to SPD$_1$, where he sifts the key by measuring time-bins. The sifting loss here is minimal, caused only by the small portion of photons routed through the phase coherence measurement path. An example histogram measured by SPD$_1$ is shown in **Figure 2**(a), giving a QBER of less than 1 %. SPD$_2$ is placed at the destructive

ADVANCED
SCIENCE NEWS
www.advancedsciencenews.com

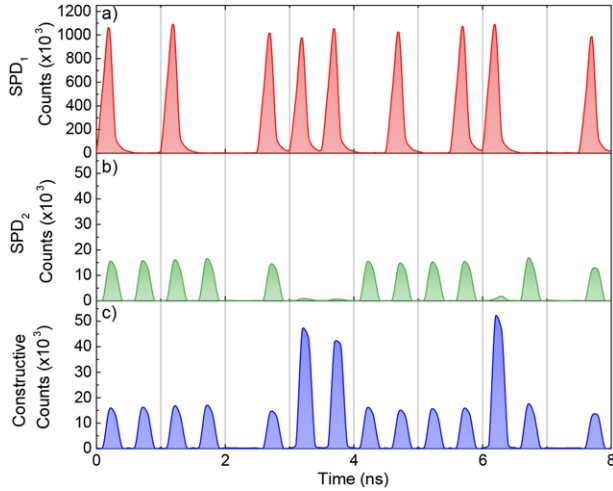LASER
& PHOTONICS
REVIEWS

www.lpr-journal.org

Figure 2. Detected signals. Complementary signals received by Bob in a) the time basis; b) the destructive arm of his interferometer; c) the constructive arm of his interferometer, measured using the SPDs. The transmitted key for these patterns is $|\beta_0\rangle$, $|\beta_0\rangle$, $|\beta_1\rangle$, $|\beta_2\rangle$, $|\beta_1\rangle$, $|\beta_1\rangle$, $|\beta_0\rangle$, $|\beta_1\rangle$, where each logical bit is separated by a vertical grey line. Data is acquired for 60 s in a quantum channel with 15 dB loss, with Alice transmitting 0.1 photons per pulse.

output port of the interferometer to enable an accurate measurement of the visibility. To highlight the interference effect, we show in Figure 2(c) an example measurement from the constructive output port of the interferometer. The height of constructive peaks is approximately four times that of the non-interfering peaks, as expected from first-order optical interference.

Each QKD session is continued until over 2×10^7 counts are collected in the time basis. The QBER and visibility are collected alongside the number of counts in each arm. The key rates are calculated using the finite key size analysis derived by Korzh *et al*[4] with a total security parameter of $\varepsilon_{QKD} = 10^{-10}$. The key rate dependence on visibility and number of photons per pulse, μ, is given by

$$\zeta = (2V - 1) \times \exp(-\mu) - 2\left\{\left[1 - \exp(-2\mu)\right] V(1 - V)\right\}^{1/2}. \tag{2}$$

The extracted key length is then calculated using

$$l = n\left[1 - Q - (1 - Q)h\left(\frac{1-\zeta}{2}\right)\right] - 7\left[n\log_2(\beta^{-1})\right]^{1/2} - f_{IR} \times h(Q) \times n - \log_2\left(\frac{1}{2\varepsilon_{cor}\beta^2}\right), \tag{3}$$

where n is the block size used for post processing, Q is the QBER, h is the binary entropy function truncated to unity at input values over 0.5, β is optimised at $\varepsilon_{QKD}/4$, f_{IR} is the efficiency of information reconciliation and ε_{cor} is the probability with which the key is incorrect. The total measurement time increases with channel attenuation, although only 600 s are required at 30 dB channel loss to collect the required number of counts.

Figure 3(a) shows the estimated secure key rate as a function of channel attenuation. This is the first time that megabit per second estimated key rates have been shown using the COW protocol. These key rates are extracted in a finite key-size scenario,
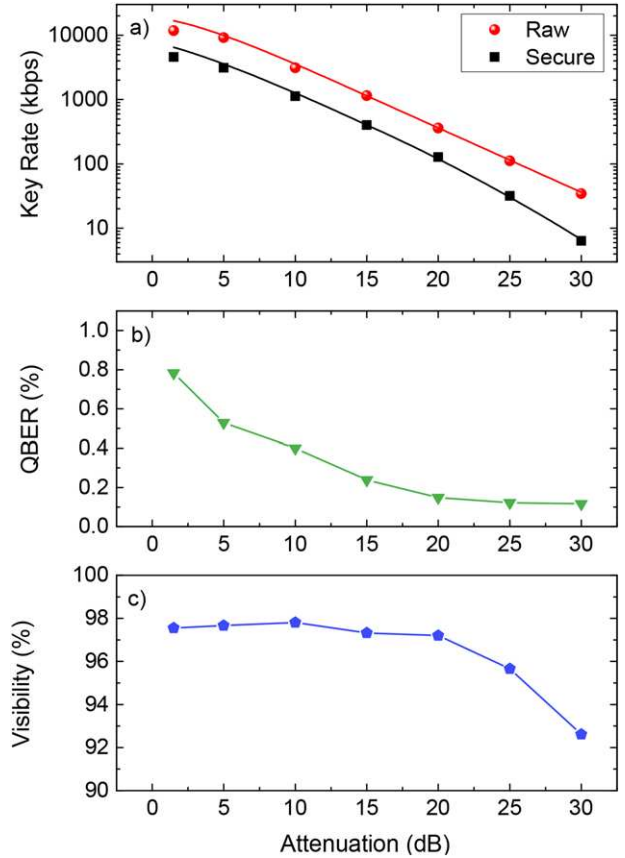

Figure 3. Experimental (symbols) and simulated (lines) key rates and associated QBERs and visibilities. COW protocol with a finite key-size analysis.[4]

attaining 4.57 Mbit/s at 1.5 dB of attenuation. As the channel attenuation increases, the secure key rate decreases exponentially. At 20 dB of optical attenuation, equivalent to 100 km of ordinary optical fiber (0.2 dB/km loss), a secure key rate of 127.8 kbps is delivered. This rate is ten times higher than that measured by Korzh *et al*[4] using the COW protocol at similar attenuations. We attribute this enhanced performance to the lower QBER enabled by our source, alongside high efficiency detectors.

We also plot the QBER and the interference visibility in Figure 3(b). These parameters give a direct evaluation of the performance of our light source as a quantum transmitter. Because the single photon detectors have negligible DCRs, we do not expect a strong variation of QBER across the entire range of the channel attenuation. This is indeed the case for attenuations equal to and above 20 dB, where the QBER is measured at below 0.15 %. This is low relative to other QKD protocols, which achieve QBERs of around 4 % at similar distances.[3,17] At the lowest channel attenuation of 1.5 dB, the QBER increases to 0.78 %. We attribute this QBER increase to the deterioration of the timing jitter performance of the superconducting nanowire detectors at high count rates, where the jitter increases from 40 ps to 90 ps. We also increase the time-bin width on the digitizer at short distances to ensure all counts are measured. This deterioration causes an overlap between the detected time-bins, as shown in Figure 2(a), creating an ambiguity in the bit value of a photon.

The interference visibility does not suffer from the time jitter deterioration because the count rate of SPD_2 is 30 times lower than SPD_1. As shown in Figure 2(b) and (c), the detection peaks are well separated from each other. We measure a visibility of 97.81 % at 10 dB attenuation, illustrating high quality coherence transfer to the intensity-modulated pulses of the slave laser. This value is lower than the master laser visibility because the direct intensity modulation slightly weakens the indistinguishability among optical pulses due to the limited bandwidth of the slave laser. While our simulations show that improvement of the visibility would only entail a relatively small increase in the secure key rates, there is potential to reach far higher modulation rates using different slave laser diodes. Transmission at 10 Gbit/s has been shown in classical communications by using a gain-switched vertical-cavity surface-emitting laser with optical injection locking.[18]

In summary, we have successfully demonstrated the suitability of a modulator-free QKD transmitter for the COW protocol. This system has produced estimated secure key rates between 4.57 Mbit/s to 6.38 kbit/s over equivalent distances of 7.5 km to 150 km. The lack of external modulators reduces both the system size and complexity. An exciting prospect opened up by this work is the potential for implementation in a multi-protocol network. Current work towards this has used bulky systems with a number of active components. The system presented in this work would enable a single transmitter to quickly switch between protocols depending on a client's requirement on bit-rate, distance or security. The wide range of functionalities offered by this transmitter, namely amplitude and phase modulation with on-demand phase randomization, mean that newly developed protocols could be easily adopted with firmware updates. An example of this would be an extension to the COW protocol that incorporates block-wise phase randomization to offer unconditional security, similar to work done for the DPS protocol.[19]

Acknowledgments

Conflict of Interest

The authors have declared no conflict of interest.

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, *Rev. Mod. Phys.* **74** (1), 145–195 (2002).

[2] E. Diamanti, H-K. Lo, B. Qi, and Z. L. Yuan, *npj Quantum Information* **2**, 16025 (2016).

[3] A. R. Dixon, Z. L. Yuan, J. F. Dynes, A. W. Sharpe, and A. J. Shields, *Appl. Phys. Lett.* **96** (16), 161102 (2010).

[4] B. Korzh, C.C.W. Lim, R. Houlmann, N. Gisin, M.J. Li, D. Nolan, B. Sanguinetti, R. Thew, and H. Zbinden, *Nat. Photonics* **9** (3), 163–168 (2015).

[5] B. Fröhlich, M. Lucamarini, J. F. Dynes, L. C. Comandar, W. W-S. Tam, A. Plews, A. W. Sharpe, Z. L. Yuan, and A. J. Shields, *Optica* **4** (1), 163, (2017).

[6] K. A. Patel, J. F. Dynes, M. Lucamarini, I. Choi, A. W. Sharpe, Z. L. Yuan, R. V. Penty, and A. J. Shields, *Appl. Phys. Lett.* **104** (5), 051123 (2014).

[7] J. Qiu, *Nature* **508**, 441, (2014).

[8] C. H. Bennett and G. Brassard, in: International Conference on Computer System and Signal Processing, IEEE, 1984, pp. 175–179.

[9] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, *Rev. Mod. Phys.* **81** (3), 1301 (2009).

[10] P. Sibson, M. Godfrey, C. Erven, S. Miki, T. Yamashita, M. Fujiwara, M. Sasaki, H. Terai, M. G. Tanner, C. M. Natarajan, R. H. Hadfield, J. O'Brien, and M. G. Thompson, *Nat. Comms.* **8**, 13984 (2017).

[11] Z. L. Yuan, B Föhlich, M Lucamarini, G. L. Roberts, J. F. Dynes, and A. J. Shields, *Phys. Rev. X* **6** (3), 031044 (2016).

[12] K. Inoue, E. Waks, and Y. Yamamoto, *Phys. Rev. Lett.* **89** (3), 037902 (2002).

[13] R. Loudon, *The quantum theory of light* (OUP Oxford, 2000).

[14] Z. Liu, J. Kakande, B. Kelly, J. O'Carroll, R. Phelan, D. J. Richardson, and R. Slavik, *Nat. Comms.* **5**, 5911 (2014).

[15] J. He, G. Jin, B. Liu and J. Wang, *Opt. Lett.* **41**, 5724 (2016).

[16] L. C. Comandar, M. Lucamarini, B. Fröhlich, J. F. Dynes, A. W. Sharpe, S.W.-B. Tam, Z. L. Yuan, R. V. Penty, and A. J. Shields, *Nat. Photonics.* **10**, 312 (2016).

[17] M. Lucamarini, K. A. Patel, J. F. Dynes, B. Fröhlich, A. W. Sharpe, A. R. Dixon, Z. L. Yuan, R. V. Penty, and A. J. Shields, *Opt. Express* **21** (21), 24550 (2013).

[18] C. C. Lin, Y. C Chi, H. C. Kuo, P. C. Peng, C. J. Chang-Hasnain, and G. R. Lin, *J. Lightw. Technol.* **29**, 830 (2011).

[19] K. Tamaki, M. Koashi, and G. Kato, arXiv preprint arXiv:1208.1995 (2012).