Monograph:

Marco, Innocenzo De, Woodward, Robert I., Roberts, George L. et al. (6 more authors) (2021) Real-time operation of a multi-rate, multi-protocol quantum key distribution transmitter. Working Paper. ArXiv e-prints .

White Rose
university consortium
Universities of Leeds, Sheffield & York

eprints@whiterose.ac.uk
https://eprints.whiterose.ac.uk/

Real-time operation of a multi-rate, multi-protocol quantum key distribution transmitter

Innocenzo De Marco,[1,2,*] Robert I. Woodward,[1] George L. Roberts,[1,3] Taofiq K. Paraïso,[1]
Thomas Roger,[1] Mirko Sanzaro,[1] Marco Lucamarini,[1] Zhiliang Yuan,[1] and Andrew J. Shields[1]

[1]*Toshiba Europe Ltd, 208 Cambridge Science Park, Cambridge, CB4 0GZ, United Kingdom*
[2]*School of Electronic and Electrical Engineering,*
University of Leeds, Leeds, LS2 9JT, United Kingdom
[3]*Cambridge University Engineering Department, 9 JJ Thomson Avenue, Cambridge, CB3 0FA, United Kingdom**

Quantum key distribution (QKD) is the best candidate for securing communications against attackers, who may in the future exploit quantum-enhanced computational powers to break classical encryption. As such, new challenges are arising from our need for large-scale deployment of QKD systems. In a realistic scenario, transmitting and receiving devices from different vendors should be able to communicate with each other without the need for matching hardware. Therefore, practical deployment of QKD would require hardware capable of adapting to different protocols and clock rates. Here, we address this challenge by presenting a multi-rate, multi-protocol QKD transmitter linked to a correspondingly adaptable QKD receiver. The flexibility of the transmitter, achieved by optical injection locking, allows us to connect it with two receivers with inherently different clock rates. Furthermore, we demonstrate the multi-protocol operation of our transmitter, communicating with receiving parties employing different decoding circuits.

I. INTRODUCTION

Quantum key distribution (QKD) allows users to communicate with information theoretical security [1]. It has become a strong candidate to resolve the imminent threat posed by quantum computers[2] to many existing cryptographic protocols based on complexity theory [3]. QKD, on the other hand, bases its security on the laws of quantum mechanics and would not be affected by the advent of quantum computers. There have been many impressive demonstrations of point-to-point QKD over fibre links, including key sharing at 10 Mbit/s [4] and at a distance of 421 km [5] for a point-to-point link of optical fibre. Such distances can be further improved thanks to the novel twin-field QKD protocol [6], which has the capability to reach more than 500 km [7, 8].

Large-scale implementations of QKD will likely see users having different devices from different manufacturers. This calls for an urgent need for interoperability. In a realistic scenario, users would likely choose their device based on required performance and system cost, where different vendors might offer devices operating at different clock rates or via different protocols. [9] Much of the current research within QKD aims at improving specific systems, while little consideration is given to interoperability between different systems. This has led to the situation where dedicated hardware is required to implement separate protocols and to operate at a fixed clock rate. Multi-rate, multi-protocol capability of the transmitters and receivers are hence highly desirable in this scenario [10, 11]. However, much of the research in this direction has focussed solely on highlighting the flexibility of the transmitter by implementing the protocols sep-

arately. In a scenario where communication with several parties is required, being able to switch between clock rates and protocols in real time is crucial for efficient communication.

In this manuscript we demonstrate real-time, multi-clock and multi-protocol continuous operation of a directly phase-modulated QKD transmitter [12, 13]. By changing only the driving signal sent to our transmitter, we are able to change its operating regime in real time to communicate with a different receiving device. The system stabilisation happens within a few seconds, without loss of integrity or degradation of the Quantum Bit Error Rate (QBER) and Secure Key Rates (SKR) afterwards.

II. EXPERIMENTAL REALISATION

Protocols We implement three QKD protocols. The first is the differential phase shift (DPS) protocol [14]. This protocol is based on the encoding of information in the phase difference of consecutive pulses. Alice can encode her information with $\{0, \pi\}$ phase shifts, and Bob will decode it using an asymmetric Mach-Zehnder interferometer (aMZI).

The second protocol is the time-bin encoded BB84 protocol [15] with decoy states [16–18]. Here, the information is carried by the phase difference in pulse pairs. Pulses belonging to different pairs need to have a random phase difference. Such randomness is necessary to minimise the amount of information an eavesdropper can retrieve from the pulse [19]. Alice encodes her qubits in two different bases: for the **X** basis, phase shifts of $\{0, \pi\}$ are used. For the **Y** basis, phase shifts of $\{\pi/2, 3\pi/2\}$ are used. The intensity of the optical pulses is modulated to implement the decoy states technique.

* innocenzo.demarco@crl.toshiba.co.uk

Finally, the last protocol we implement is the Coherent One Way (COW) protocol [20]. The information is encoded in the time bins of pulse pairs, the coherence between which is used to check whether these pulses have been tampered with.

As a proof-of-principle demonstration, we consider the protocols' asymptotic secure key rates. A full finite-size analysis is outside the scope of the present paper and would not change the significance of our results. Moreover, to simplify the data collection, data is collected in one basis only for the BB84 protocol, with the assumption that the two bases are chosen with identical probabilities and have similar phase errors. Finally, since the data is recorded and measured as a cumulative histogram of a repeating pattern, one detector is sufficient to measure the QBER. This all means that we only need one detector for the BB84 and DPS protocols and two detectors for the COW protocol (one for the time-bin encoding, one for decoy detection). This also means that the same receiver can be used for all three protocols at a given clock rate. The input of the chip is split between the straight waveguide and the interferometer, with a ∼ 50 : 50 splitting ratio, which allows us to measure all the quantities we need at once. While not the case in a realistic scenario, this is reasonable for a proof of principle experiment as we are able to extract all the needed information from this simplified setup.

It is important to note that security proofs for the three protocols show that they have significant differences in their security. For example, the decoy-state BB84 protocol is secure against coherent attacks, whereas the security proofs for the DPS and COW protocols are based on collective attacks. For this reason, the comparison between the SKRs obtained with the BB84 [21], DPS [22] and COW [23] protocols should be taking this into account.

Modulator-free transmitter The encoding is based on the combination of two well-known techniques in laser physics: optical injection locking (OIL) [24, 25] and direct phase modulation [26]. This approach has been proven to effectively remove the need for a phase modulator in QKD [12]: this makes our transmitter versatile while also reducing the number of optical elements in the setup. Another advantage of our transmitting setup is the lack of an aMZI. This is useful for two main reasons: first of all, this greatly reduces losses since there is no mismatch between two arms of different length. In a fibre-based system this does not have a big impact, but chip-based experiments suffer from higher losses, hence a 500 ps or 1 ns delay line would lead to a power mismatch between the two arms. For this reason, chip-based experiments usually avoid embedding an aMZI in the transmitter, resorting to modulating every pulse with a phase modulator [11] or exploiting the directly phase-modulated setup [13]. The second advantage of an aMZI-free setup is the ability to use the same setup to encode different protocols. This is crucial to our experiment, as it allows us to change different protocols and/or clock rates at will by simply changing the modulation of the driving current, with a transient of less than 5 seconds between every change.

The experimental setup is shown in Fig. 1. We use arbitrary waveform generators (AWG) with a sampling rate of 24 Gs/s and vertical resolution of 8 bit to drive the lasers at GHz clock rates and synchronise the system. A phase encoding laser injects light into a second, injection locked laser through a circulator. These are both discrete optics, off-the-shelf DFB lasers, with a bandwidth of ¿10 GHz. An intensity modulator sets the signal and decoy levels for the system. The quantum channel is simulated by a variable optical attenuator (VOA), fibre-coupled to the transmitter and the receiver. A MEMS switch is used to select the correct receiver chip, according to the driving signal sent to the transmitter setup. At the output of the receiver chips, optical fibres are coupled to superconducting nanowire single photon detectors (SNSPDs) [27]; each of the outputs (the time-bin encoding waveguide for COW and one of the interferometer outputs for all three protocols, as mentioned in the previous paragraph) is connected to a detector. The SNSPDs' output is read by a single-photon counting module (SPCM) which digitises the data and sends the results to Bob's computer where the QBER and key rates are computed.

We encode our information as shown in Fig 2. For the COW and DPS protocol, the phase encoding laser is always biased over its threshold to produce continuous-wave (CW) emission; additionally, in the DPS case, a small current modulation, synchronised to the interval of two injection locked pulses, is applied when a π phase modulation is required. The BB84 protocol requires, in addition to the phase modulation, a random global phase: only pulses belonging to the same pair of time-bins have a set phase difference. To this end, the phase encoding laser is driven periodically above and below the lasing threshold, exploiting the inherent randomness of gain-switching [28, 29].

Integrated receivers The receivers are SiO_xN_y photonic chips, whose interferometer length determine the clock rates they work at. We use receiver chips whose interferometer delay lengths are 500 ps and 400 ps, achieving clock rates of 2 and 2.5 GHz respectively.

Our QKD receivers are manufactured on a silicon-based substrate, which allows for low losses and easy integration. Our receiver chips are designed to have different interferometers, each one decoding information for a different protocol.

The interferometers are tuned by means of thermo-optic phase shifters. Such elements can be driven with a DC current source; a π phase shift is obtained with a voltage of around 15 V. The phase shift induced by the heaters can be used to direct light towards one arm or the other of the interferometer, or to balance the power between the two arms. This is particularly important since the long arm will cause a power imbalance at the output coupler: the length of the delay line will cause
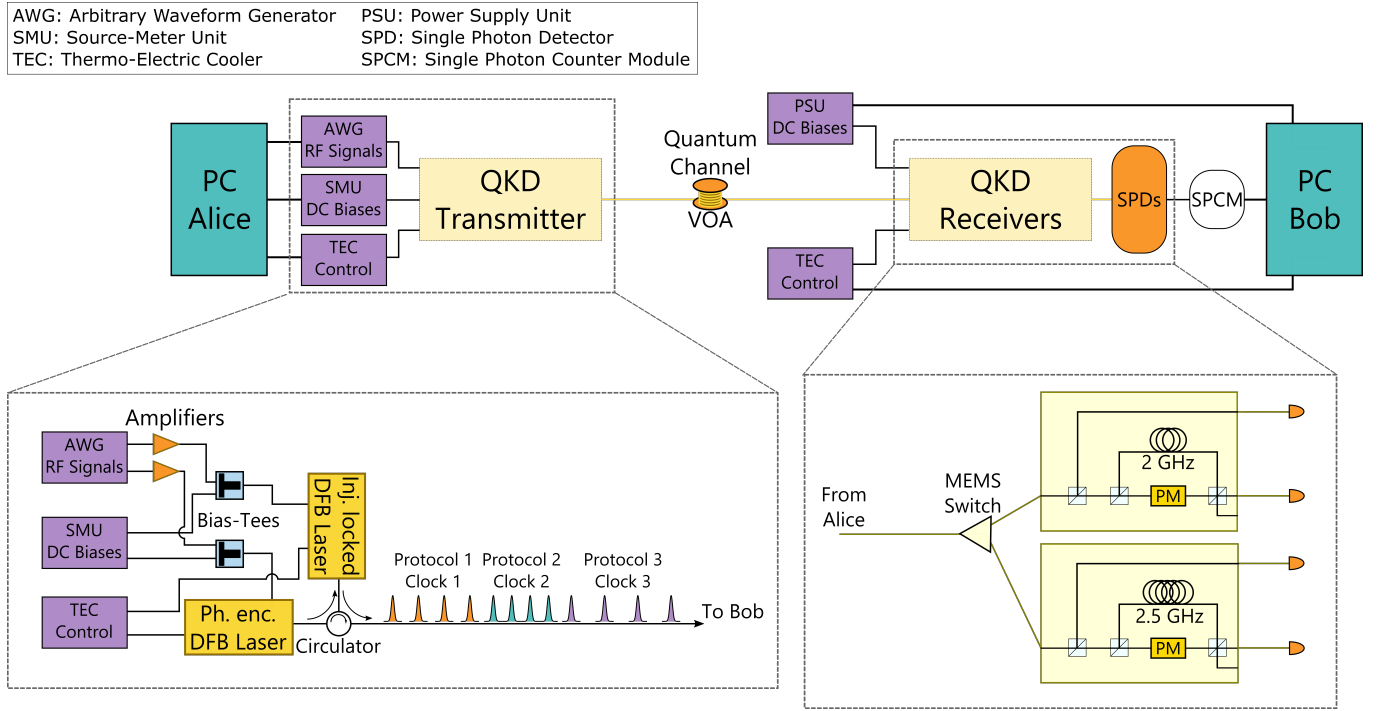
FIG. 1. **Experimental setup** Schematic of the experimental setup used to carry out the experiment. DC and RF signals are combined through a bias-tee and sent to the phase encoding and injection locked lasers. A circulator prevents light from the latter going back to the phase encoding laser. The RF signals are changed to encode different protocols and clock rates. An optical MEMS switch selects the correct receiver chip, which is out-coupled to SNSPDs.

more losses. For this experiment, the total loss for the interferometer circuit on the 2.5 GHz chip is measured to be 10.1 dB, while the loss for the 2 GHz chip is 6.7 dB. The straight waveguides used for the COW protocol have losses that are ∼ 3 dB less than the interferometer ones.

The main contribution to the losses is the propagation loss (∼ 0.2 dB/cm) in the delay line, however a big contribution is also coming from fabrication imperfections and fibre coupling. All these cause the excess loss in the 2.5 GHz chip compared to the 2 GHz chip, as the statistical imperfections of that chip cause losses that overweigh the lower loss coming from the shorter delay line.

The output waveguides are out-coupled through optical fibres to SNSPDs, with an efficiency of 44% and dark count rates of ∼ 10 Hz.

III. RESULTS

Fig. 3 shows the performance of the transmitter at two different clock rates using the BB84 protocol. The loss considered in the plots includes only the quantum channel attenuation and the loss from the optical switch. As shown in the figure, the 2.5 GHz performs worse than the 2 GHz receiver at the same channel loss. This is due to the excess losses in the chip mentioned in the previous paragraph. The top axis of Fig. 3 shows instead the total loss, including the receiver chip loss. This allows a

clearer comparison between the chips, and shows how the higher clock rate would indeed yield a higher key rate as expected, if the chips had equal loss.

We then proceed to the main goal of the paper, demonstrating the flexibility of our system. Our transmitter is set to implement different protocols at different clock rates. A signal is then sent to the system, triggering the clock rate and protocol change after 10 minutes. When this happens, a first point is recorded with a high QBER and, consequently, no positive key rate. The main reason behind this is that the AWG's electronics takes some time to settle to a stable output. This time is below 5 seconds. Results are shown in Fig. 4. The stability of the system allows for a reasonably constant secure key rate (SKR) during a 10-minute time window, at a channel loss of 14 dB.

The QBER is stable around values of 2.7% for BB84 at both clock rates and DPS, while it is around 0.7% for the COW protocol, due to the absence of phase errors in this protocol. This yields key rates of 0.5, 0.4 and 2.5 Mbps for BB84, DPS and COW, respectively.

IV. CONCLUSION

Our experiments show the feasibility of having a single transmitter communicating with receivers employing different clock rates and protocols. This is possible be-
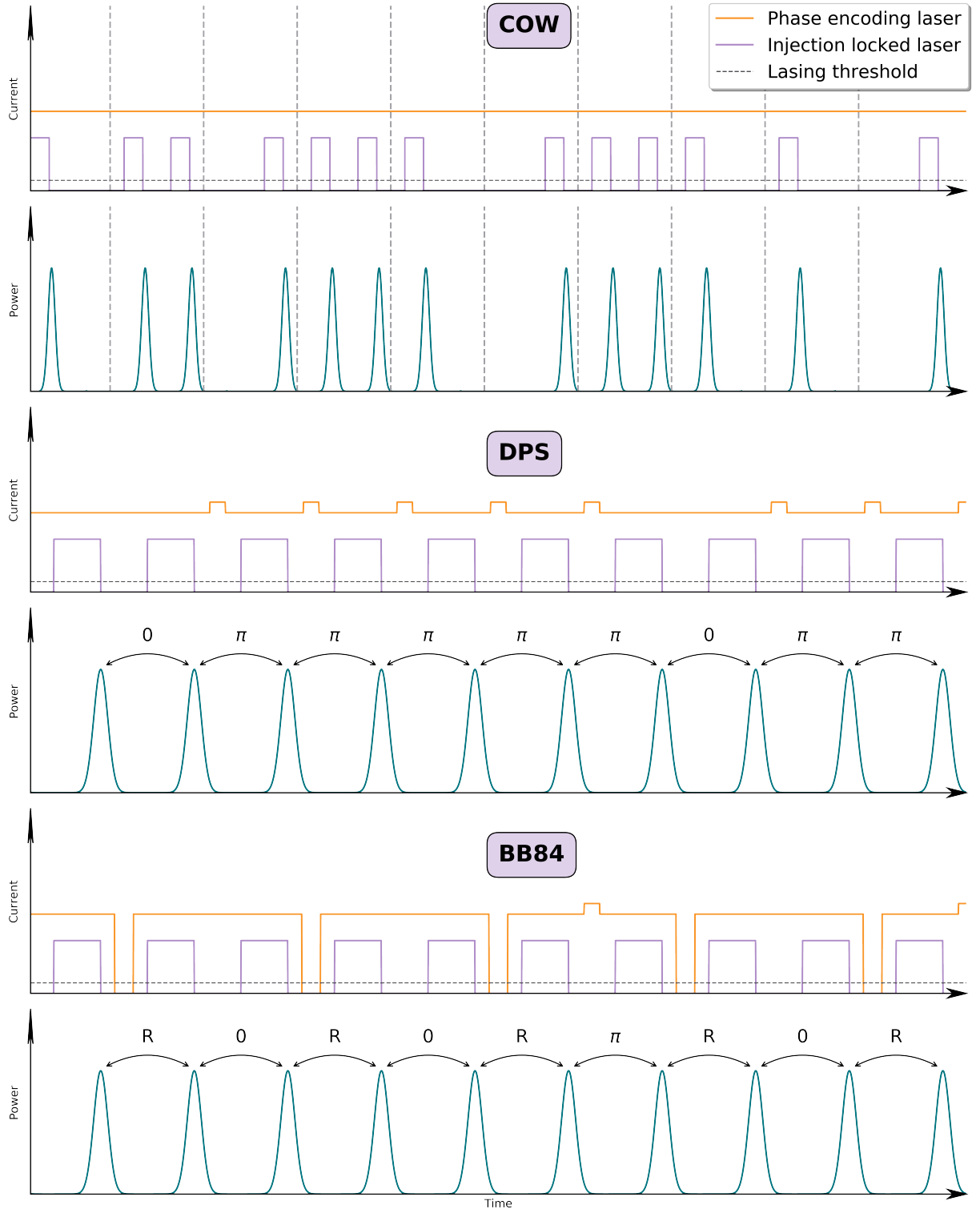
FIG. 2. **Modulation signals** Driving signals from phase encoding and injection locked lasers for the COW, DPS and BB84 protocols. For each protocol, the top plot represents the electrical driving signals, the bottom plot represents the optical output. The symbol between consecutive pulses represents the relative phase difference, where "R" refers to a random phase difference between pulses.
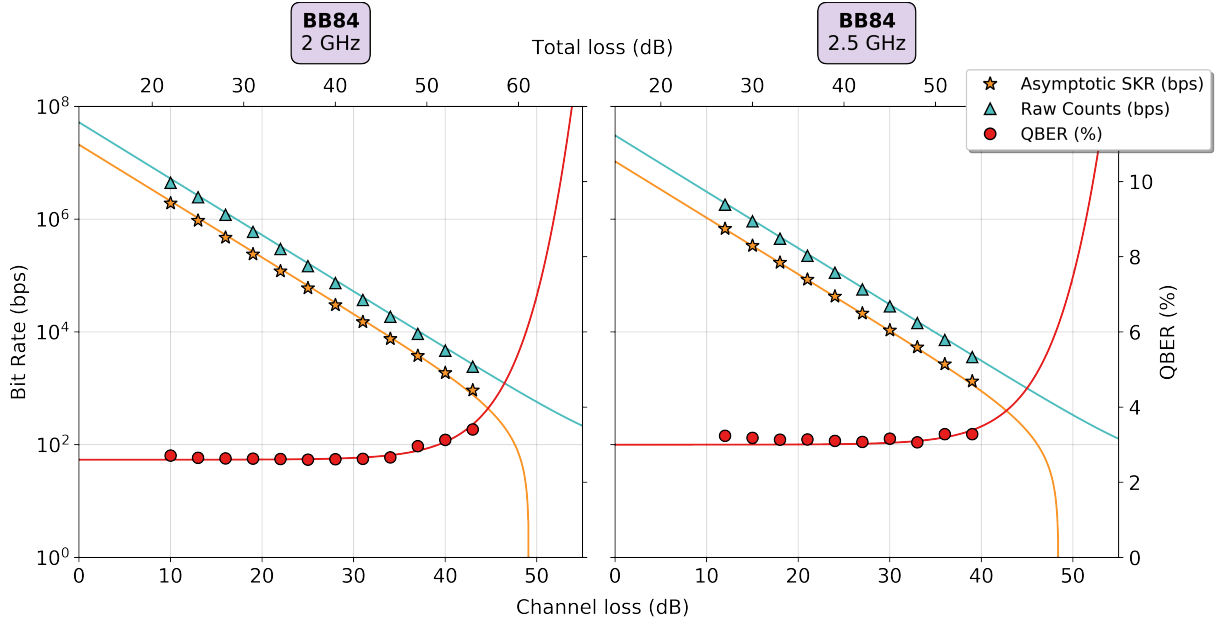
FIG. 3. **Secure key rates** BB84 secure key rates and QBER vs channel loss for 2 GHz and 2.5 GHz. The color red indicates the QBER, teal the raw count rates and orange the SKR. The points correspond to measured data, the line to the simulated behaviour.
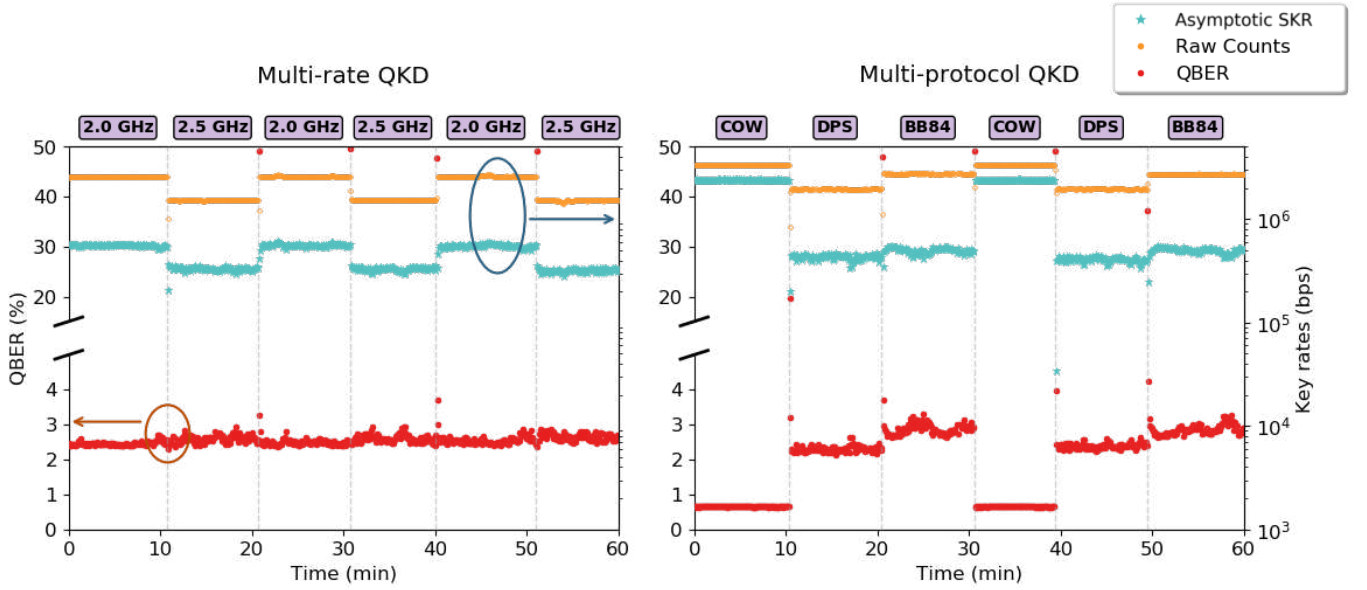

FIG. 4. **Performance of the universal transmitter** Results obtained encoding the BB84 protocol at different clock rates (left) and encoding different protocols at a 2 GHz rate (right). The first point after every change of clock rate or protocol, with a high QBER, does not result in a positive SKR. The data is collected at a channel loss of 14 dB. The 2.5 GHz regime has lower count rates than the 2 GHz regime due to the higher losses in the receiver chip.

cause of the directly phase-modulated setup which allows flexibility to change the operating conditions by simply modifying the electrical driving signals. The protocols and clock rates are set up to continuously change, leading to the system reconfiguring in real time while still maintaining a low QBER and high SKR. We showed an effective setup time lower than 5 s. This was limited by

the driving electronics, mainly the AWG, needing time to settle to the desired operation regime. Reduced times can be certainly obtained by using faster driving electronics, for instance, a custom-designed FPGA board.

On the receiver side, two different chips were used for the two different clock rates. Tuneable delay length can be considered in order to demonstrate multi-rate capabil-

ities of the receiver, however it must be noted that adding reconfigurable components would add to the complexity of the chip and could cause issues such as thermal fluctuations. An alternative approach, since the advantage of integrated photonics lies in the compactness of devices, might be to implement different interferometers on the same chip.

Our result is a step forward towards interoperability between devices from different vendors and paves the way for large-scale, collaborative deployment of QKD systems. In this respect, we believe that our work will have a positive impact on the on-going efforts in QKD standardization.

DISCLOSURES

The authors declare no conflicts of interest.

DATA AVAILABILITY

Data underlying the results presented in this paper are not publicly available but may be obtained from the authors upon reasonable request.

[1] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, The security of practical quantum key distribution, Rev. Mod. Phys. **81**, 1301 (2009).

[2] F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, R. Barends, R. Biswas, S. Boixo, F. G. S. L. Brandao, D. A. Buell, B. Burkett, Y. Chen, Z. Chen, B. Chiaro, R. Collins, W. Courtney, A. Dunsworth, E. Farhi, B. Foxen, A. Fowler, C. Gidney, M. Giustina, R. Graff, K. Guerin, S. Habegger, M. P. Harrigan, M. J. Hartmann, A. Ho, M. Hoffmann, T. Huang, T. S. Humble, S. V. Isakov, E. Jeffrey, Z. Jiang, D. Kafri, K. Kechedzhi, J. Kelly, P. V. Klimov, S. Knysh, A. Korotkov, F. Kostritsa, D. Landhuis, M. Lindmark, E. Lucero, D. Lyakh, S. Mandrà, J. R. McClean, M. McEwen, A. Megrant, X. Mi, K. Michielsen, M. Mohseni, J. Mutus, O. Naaman, M. Neeley, C. Neill, M. Y. Niu, E. Ostby, A. Petukhov, J. C. Platt, C. Quintana, E. G. Rieffel, P. Roushan, N. C. Rubin, D. Sank, K. J. Satzinger, V. Smelyanskiy, K. J. Sung, M. D. Trevithick, A. Vainsencher, B. Villalonga, T. White, Z. J. Yao, P. Yeh, A. Zalcman, H. Neven, and J. M. Martinis, Quantum supremacy using a programmable superconducting processor, Nature **574**, 505 (2019).

[3] P. W. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, SIAM review **41**, 303 (1999).

[4] Z. Yuan, A. Plews, R. Takahashi, K. Doi, W. Tam, A. Sharpe, A. Dixon, E. Lavelle, J. Dynes, A. Murakami, M. Kujiraoka, M. Lucamarini, Y. Tanizawa, H. Sato, and A. J. Shields, 10-mb/s quantum key distribution, Journal of Lightwave Technology **36**, 3427 (2018).

[5] A. Boaron, B. Korzh, R. Houlmann, G. Boso, D. Rusca, S. Gray, M.-J. Li, D. Nolan, A. Martin, and H. Zbinden, Simple 2.5 ghz time-bin quantum key distribution, Applied Physics Letters **112**, 171108 (2018).

[6] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, Overcoming the rate–distance limit of quantum key distribution without quantum repeaters, Nature **557**, 400 (2018).

[7] M. Minder, M. Pittaluga, G. L. Roberts, M. Lucamarini, J. F. Dynes, Z. L. Yuan, and A. J. Shields, Experimental quantum key distribution beyond the repeaterless secret key capacity, Nature Photonics **13**, 334 (2019).

[8] X.-T. Fang, P. Zeng, H. Liu, M. Zou, W. Wu, Y.-L. Tang, Y.-J. Sheng, Y. Xiang, W. Zhang, H. Li, Z. Wang, L. You, M.-J. Li, H. Chen, Y.-A. Chen, Q. Zhang, C.-Z. Peng, X. Ma, T.-Y. Chen, and J.-W. Pan, Implementation of quantum key distribution surpassing the linear rate-transmittance bound, Nature Photonics **14**, 422 (2020).

[9] S. Moseley, S. Randall, and A. Wiles, In pursuit of interoperability, International Journal of IT Standards and Standardization Research **2**, 34 (2004).

[10] B. Korzh, N. Walenta, R. Houlmann, and H. Zbinden, A high-speed multi-protocol quantum key distribution transmitter based on a dual-drive modulator, Optics Express **21**, 19579 (2013).

[11] P. Sibson, J. E. Kennard, S. Stanisic, C. Erven, J. L. O'Brien, and M. G. Thompson, Integrated silicon photonics for high-speed quantum key distribution, Optica **4**, 172 (2017).

[12] Z. L. Yuan, B. Fröhlich, M. Lucamarini, G. L. Roberts, J. F. Dynes, and A. J. Shields, Directly phase-modulated light source, Physical Review X **6**, 031044 (2016).

[13] T. K. Paraïso, I. De Marco, T. Roger, D. G. Marangon, J. F. Dynes, M. Lucamarini, Z. Yuan, and A. J. Shields, A modulator-free quantum key distribution transmitter chip, npj Quantum Information **5**, 42 (2019).

[14] K. Inoue, E. Waks, and Y. Yamamoto, Differential-phase-shift quantum key distribution using coherent light, Physical Review A **68**, 022317 (2003).

[15] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, in *International Conference on Computer System and Signal Processing, IEEE, 1984* (1984) pp. 175–179.

[16] H.-K. Lo, X. Ma, and K. Chen, Decoy state quantum key distribution, Physical Review Letters **94**, 230504 (2005).

[17] W.-Y. Hwang, Quantum key distribution with high loss: Toward global secure communication, Physical Review Letters **91**, 057901 (2003).

[18] X.-B. Wang, Beating the photon-number-splitting attack in practical quantum cryptography, Physical Review Letters **94**, 230503 (2005).

[19] H.-K. Lo and J. Preskill, Security of quantum key distribution using weak coherent states with nonrandom phases, Quantum Information & Computation **8**, 431 (2007).

[20] D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, Fast and simple one-way quantum key distribution, Applied Physics Letters **87**, 194108 (2005).

[21] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, Practical decoy state for quantum key distribution, Physical Review A **72**, 012326 (2005).

[22] E. Waks, H. Takesue, and Y. Yamamoto, Security of differential-phase-shift quantum key distribution against individual attacks, Physical Review A **73**, 012344 (2006).

[23] D. Stucki, C. Barreiro, S. Fasel, J.-D. Gautier, O. Gay, N. Gisin, R. Thew, Y. Thoma, P. Trinkler, F. Vannel, *et al.*, Continuous high speed coherent one-way quantum key distribution, Optics Express **17**, 13326 (2009).

[24] N. Le Binh, *Optical modulation: Advanced techniques and applications in transmission systems and networks*, Optical science and engineering (Taylor & Francis a CRC title part of the Taylor & Francis imprint a member of the Taylor & Francis Group the academic division of T&F Informa plc, Boca Raton, 2018).

[25] N. P. Barnes and J. C. Barnes, Injection seeding i: Theory, IEEE Journal of Quantum Electronics **29**, 2670 (1993).

[26] M. Shirasaki, H. Nishimoto, T. Okiyama, and T. Touge, Fibre transmission properties of optical pulses produced through direct phase modulation of dfb laser diode, Electronics Letters **24**, 486 (1988).

[27] Chandra M. Natarajan, Michael G. Tanner, and Robert H. Hadfield, Superconducting nanowire single-photon detectors: Physics and applications, Superconductor Science and Technology **25**, 063001 (2012).

[28] M. Jofre, M. Curty, F. Steinlechner, G. Anzolin, J. P. Torres, M. W. Mitchell, and V. Pruneri, True random numbers from amplified quantum vacuum, Optics Express **19**, 20665 (2011).

[29] Z. L. Yuan, M. Lucamarini, J. F. Dynes, B. Fröhlich, A. Plews, and A. J. Shields, Robust random number generation using steady-state emission of gain-switched laser diodes, Applied Physics Letters **104**, 261112 (2014).