Cavity integrated quantum key distribution

Darius Bunandar,[1,*] Nicholas Harris,[1,†] Zheshen Zhang,[1] Catherine Lee,[1] Ran Ding,[2] Tom Baehr-Jones,[2] Michael Hochberg,[2] Jeffrey Shapiro,[1] Franco Wong,[1] and Dirk Englund[1]

[1] *Research Laboratory of Electronics, Massachusetts Institute of Technology, Cambridge, Massachusetts 02139, USA*
[2] *Coriant Advanced Technology Group, 1415 West Diehl Road, Naperville, Illinois 60563, USA*

(Dated: April 29, 2016)

We present a scalable Quantum Key Distribution (QKD) transmitter based on an integrated ring cavity that directly enables high-rate quantum communications that take advantage of parallelism enabled by wavelength-division multiplexing. The ring cavity modulates single photons using the plasma dispersion effect when current is injected into the p-i-n junction surrounding the cavity. To demonstrate the system's feasibility, we generated secret keys using the coherent-one-way protocol at a rate higher than 236 kbps in a field test between two different laboratories at MIT.

Recent QKD demonstrations have shown secret-key rates at Mbps [1–5], but a large gap exists between QKD and today's classical telecommunication systems which operate at rates of 1 Gbps between end users. Bridging this gap is necessary for enabling quantum secure communication systems that can be used to safely transmit large sensitive data in the future. Future QKD systems can, therefore, benefit from exploiting previously unused degrees of freedom of light such as wavelength. In a wavelength-division multiplexed (WDM) QKD system, parallel QKD systems operating at different wavelength channels can generate secret keys concurrently through a single optical fiber [6].

We demonstrate the design of a QKD transmitter based on an integrated ring cavity in a silicon photonic integrated circuit (PIC), which is a dominant platform for optical communications. The transmitter is shown in Figure 1. The near critically-coupled ring cavity has a diameter of 30 μm, a free-spectral range (FSR) of 6 nm, and a quality factor of 6279. Integrated ring cavities act as light-confining structures that enhance the effects of refractive index change on the transmission response. The transmission through the ring is high when the laser wavelength is resonant with the ring, specifically when the ring circumference corresponds to an integer number of the guided light wavelength. The resonant frequency of the ring cavity can be redshifted using the thermo-optic heater which increases the cavity optical path length when the cavity is being heated. The wavelength-selective—and tunable—property of ring cavities makes them particularly suitable for building WDM QKD transmitters, as shown in Figure 2.

Extinction ratio—the ratio of power between the modulator's on-state and its off-state—is a critical metric in quantum cryptography systems, since it is the probability of a single photon entering the quantum channel when the modulator is in its off-state. If this photon is detected by Bob's apparatus, it can not only cause an error in Bob's measurement, but also render Bob's detector inactive for the reset time duration. Modulation in a PIC is typically achieved by producing a refractive index change in the waveguide, and the amount of refractive index change depends strongly on the amount of electro-optic effect that can be provided within the system [7, 8]. The cavity-based design of our QKD transmitter enhances this electro-optic effect by confining the light within a cavity, such that any refractive index change on the cavity is amplified by the number of round trips the light travels around the cavity. Therefore, the footprint of the ring cavity QKD transmitter can be maintained to within tens of μm in diameter.

We achieve a high extinction ratio of more than 16 dB by leveraging the plasma dispersion effect [9] in a boron-phosphorus doped silicon junction that overlaps the optical mode, as shown in Figure 1(a). Typically, ring cavity modulators deplete charge carriers (electrons and holes) from the guided region; we, instead, inject charge carriers—providing higher extinction ratio, but at the cost of limiting the modulator rate by the carrier recombination time of the silicon sample (typically on the order of a nanosecond). Further improvements to the extinction ratio can be achieved by incorporating more than one cavity, placed within one diameter apart, to carve the same light pulse.

To demonstrate the feasibility of the integrated ring cavity, we performed a QKD field test between the Compton Laboratories (Building 26) and the Fairchild Building (Building 36) at MIT. Our system, shown in Figure 1, implements the coherent-one-way QKD protocol [10], where bit string is encoded in the arrival time of the weak coherent pulses modulated by the ring cavity. Furthermore, channel disturbance, which we assume to be due to Eve, is monitored by measuring the visibility of the interference between two adjacent pulses.

Alice randomly prepares the state $|\mathbf{0}\rangle = |\alpha\rangle_0 |0\rangle_1$ and $|\mathbf{1}\rangle = |0\rangle_0 |\alpha\rangle_1$ to send bits 0 and 1 respectively, where $|\alpha\rangle_i$ represents a laser pulse in time bin i. Alice further prepares decoy state $|\mathbf{d}\rangle = |\alpha\rangle_0 |\alpha\rangle_1$ randomly to monitor the phase coherence of two consecutive laser pulses. Bob, on the other hand, uses an asymmetric beamsplitter to randomly choose one of the two possible measurement bases: arrival-time or interference. In the arrival-time ba-

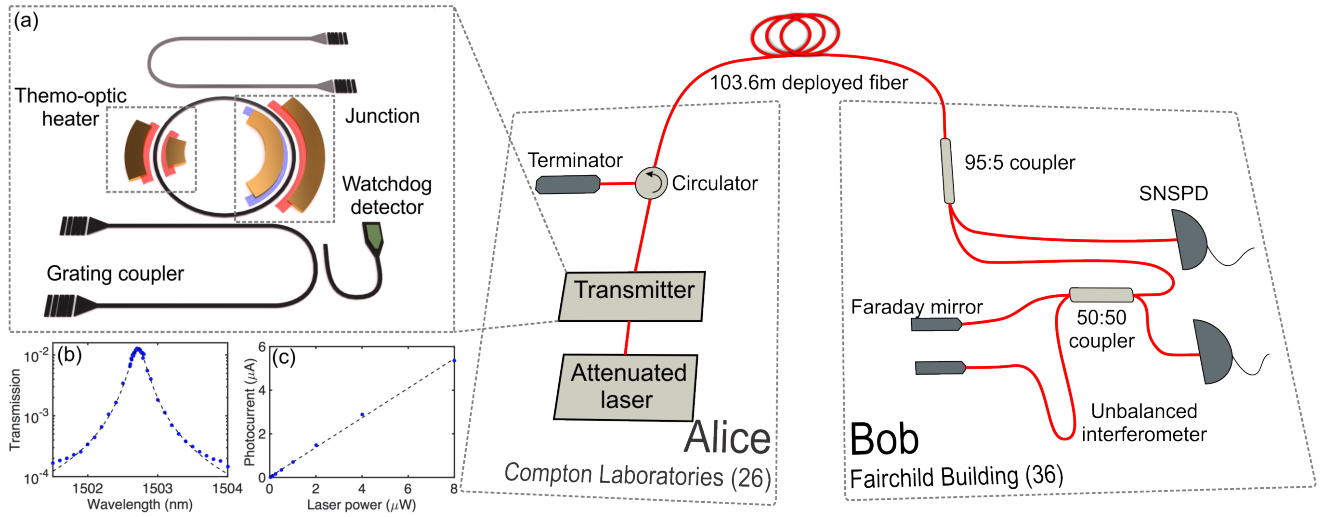

FIG. 1. Experimental setup of the cavity integrated QKD field test. Alice's attenuated laser is modulated by integrated cavity in Compton Laboratories. Bob's setup, located in Fairchild Building, performs an asymmetric basis choice between the arrival-time basis and the interference basis. For each basis choice, Bob uses a WSi superconducting nanowire single-photon detector (SNSPD) with 85% quantum efficiency. *Inset (a):* Schematic diagram of the cavity integrated QKD transmitter. The germanium watchdog detector is used to prevent Eve from sending Trojan photons into the transmitter. *Inset (b):* Transmission through the ring cavity at center wavelength of 1502.72 nm. *Inset (c):* Detector's photocurrent response to input laser power. Dashed (black) line is a linear fit to the photodiode response.

sis, Bob directly measures the arrival time of the incoming laser pulses and generates a raw bit string. The quantum bit error rate (QBER), denoted by $\hat{Q}$, can be measured without any uncertainty by counting the number of bits flipped between Alice's and Bob's raw bit strings. In the interference basis, Bob first passes two adjacent pulses through an unbalanced Michelson interferometer before measuring the resulting interference. The phase of the interferometer is maintained such that Bob measures the destructive port of the interferometer. The visibility of the interference can be measured by comparing detections due to interfering events (two adjacent pulses) and non-interfering events (single pulse). The quantum visibility V_{key} used to generate the secret keys is estimated by bounding $V_{\text{key}} \leq \hat{V} = V_{\text{obs}} - t$, where V_{obs} is the observed visibility and t is a positive parameter related to the estimation procedure [11].

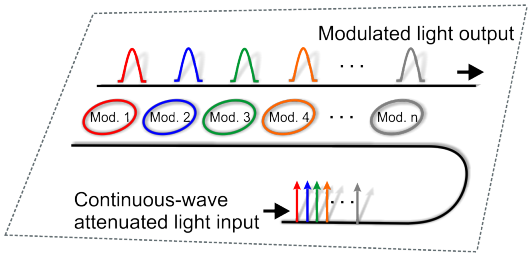

FIG. 2. Schematic of a WDM QKD transmitter with n spectral channels. Parallel spectral channels are modulated concurrently—each by a cavity modulator—and transmitted through a single output.

Moreover, Alice also prevents the Trojan-horse attack by monitoring the photocurrent generated by the germanium photodiode to sense any possible counter-propagating light into her transmitter. If Alice detects such counter-propagating light, she then aborts the QKD protocol—deeming it insecure against Eve's eavesdropping attempts. Alice's watchdog detector has a bandwidth of above 30 GHz and a responsivity of 0.68 A/W.

Alice and Bob then distill a secret key length ℓ from a weakly random bit string of length n for some security parameter ϵ and mean photon number per pulse μ. The secret key length can be bounded by

$$\ell \leq n\left[1 - fh(\hat{Q}) - \hat{Q} - (1-\hat{Q})h\left(\frac{1+\xi(\mu,\hat{V})}{2}\right)\right] - 7\sqrt{n\log_2\frac{1}{\epsilon}} - \log_2\frac{1}{2\epsilon^3}, \quad (1)$$

where $h(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is the binary Shannon entropy, and $\xi(\mu,\hat{V}) = (2\hat{V}-1)e^{-\mu} - 2\sqrt{\hat{V}(1-\hat{V})(1-e^{-2\mu})}$ [11, 12]. In estimating the key rate, we take $f = 1.2$. Furthermore, we adopt a tight failure probability $\epsilon_{\text{qkd}} = 4\times10^{-9}$ with $\epsilon_{\text{cor}} = \epsilon_{\text{sec}} = \epsilon = 10^{-9}$, where ϵ_{cor} is the probability of Alice and Bob having nonidentical secret keys and ϵ_{sec} is the probability of their secret keys being distinguishable from ideal secret keys.

Figure 3 shows the secret key rates (SKRs) of our QKD system, along with the measured QBER $\hat{Q}$ and visibil-

ity $\hat{V}$. We calculated the SKRs not only in the composable security framework, but also in the asymptotic limit to compare the performance of our current physical QKD system to the performance of the system if Alice and Bob had access to an unlimited amount of resources. Furthermore, to test the performance of our system when operating with longer quantum channels, we added fiber spools of lengths up to 31.5 km in increments of 10.5 km. The mean photon number is maintained at 0.0487 per pulse at all distances to avoid saturating Bob's detectors, and we obtained the highest SKR of 236.5 kbps at a distance of 103.6 m.

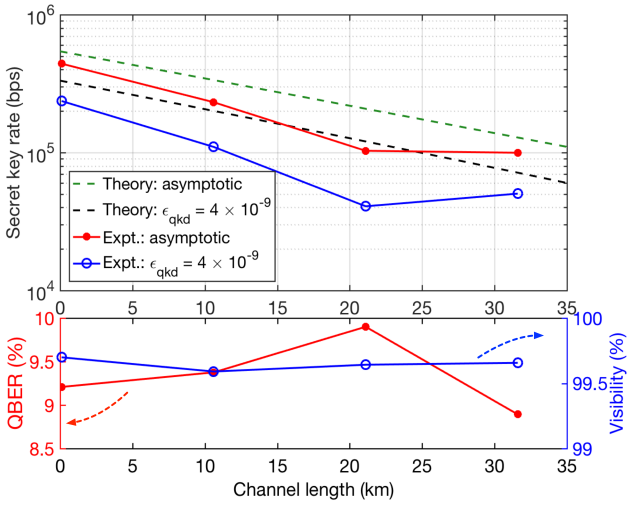

FIG. 3. *Top panel:* Final experimental SKR results plotted against fiber-optic channel length. The solid (red) circles are the calculated SKR in the asymptotic regime, while the empty (blue) circles are the calculated SKR using the composable security framework with $\epsilon_{\text{qkd}} = 4 \times 10^{-9}$. The dashed (green and black) lines are the theoretical plots for the two aforementioned SKR calculation frameworks, assuming 0.2 dB/km attenuation over the fiber-optic quantum channel. *Bottom panel:* QBER, $\hat{Q}$ (solid red circles), and visibility, $\hat{V}$ (empty blue circles), measured at each channel length.

We present a scalable QKD transmitter based on an integrated ring cavity on a silicon photonics chip that is directly designed to eventually exploit the multi-wavelength parallelism enabled in WDM QKD systems. This work establishes the feasibility of the integrated ring cavity QKD transmitter by performing a QKD field test between two different laboratories. We achieved an SKR of better than 236 kbps at a distance of 103.6 m with a tight failure probability of $\epsilon_{\text{qkd}} = 4 \times 10^{-9}$. The cavity transmitter's small size (30 μm in diameter) makes it ideal to be spectrally multiplexed in a scalable manner: a single silicon photonics chip with a footprint of less than 0.1 mm^2 could, in principle, carry more than 100 such cavity transmitters to boost the rate of secret key generation to that commensurate with today's classical telecommunication rate.

The authors would like to thank Charles Lim Ci Wen, Xuhong Zhang, Feihu Xu, and Gregory Steinbrecher for their helpful discussions. Furthermore, the authors would like to acknowledge the assistance provided by Adrian Pyke of Sanchez Microelectronics in wire bonding electrical interconnections to the ring cavity. This work was supported by the Samsung Global Research Outreach Program in quantum information.

* dariusb@mit.edu
† n_h@mit.edu

[1] Q. Zhang, H. Takesue, T. Honjo, K. Wen, T. Hirohata, M. Suyama, Y. Takiguchi, H. Kamada, Y. Tokura, O. Tadanaga, Y. Nishida, M. Asobe, and Y. Yamamoto, New Journal of Physics **11** (2009), 10.1088/1367-2630/11/4/045010, arXiv:0809.4018.

[2] E. A. Dauler, N. W. Spellmeyer, A. J. Kerman, R. J. Molnar, K. K. Berggren, and D. John, Quantum Electronics and Laser Science Conference , QTHI2 (2010).

[3] M. Lucamarini, K. A. Patel, J. F. Dynes, A. W. Sharpe, Z. L. Yuan, R. V. Penty, and A. J. Shields, Optics Express **21**, 24550 (2013), arXiv:arXiv:1302.4139.

[4] L. C. Comandar, B. Fröhlich, M. Lucamarini, K. A. Patel, A. W. Sharpe, J. F. Dynes, Z. L. Yuan, R. V. Penty, and A. J. Shields, Applied Physics Letters **104**, 16 (2014), arXiv:1402.2210.

[5] T. Zhong, H. Zhou, R. D. Horansky, C. Lee, V. B. Verma, A. E. Lita, A. Restelli, J. C. Bienfang, R. P. Mirin, T. Gerrits, S. W. Nam, F. Marsili, M. D. Shaw, Z. Zhang, L. Wang, D. Englund, G. W. Wornell, J. H. Shapiro, and F. N. C. Wong, New Journal of Physics **17**, 22002 (2015).

[6] K.-i. Yoshino, T. Ochi, and M. Fujiwara, Optics Express **21**, 6 (2013), arXiv:1308.1011.

[7] T. Baehr-Jones, R. Ding, Y. Liu, A. Ayazi, T. Pinguet, N. C. Harris, M. Streshinsky, P. Lee, Y. Zhang, A. E.-J. Lim, T.-Y. Liow, S. H.-G. Teo, G.-Q. Lo, and M. Hochberg, Optics Express **20**, 12014 (2012).

[8] J. Leuthold, C. Koos, and W. Freude, Nature Photonics **4**, 535 (2010).

[9] R. A. Soref and B. R. Bennett, IEEE Journal of Quantum Electronics **23**, 123 (1987).

[10] D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, Applied Physics Letters **87**, 1 (2005), arXiv:0506097 [quant-ph].

[11] B. Korzh, C. C. W. Lim, R. Houlmann, N. Gisin, M. J. Li, D. Nolan, B. Sanguinetti, R. Thew, and H. Zbinden, Nature Photonics **9**, 7 (2014), arXiv:1407.7427.

[12] N. Walenta, A. Burg, D. Caselunghe, J. Constantin, N. Gisin, O. Guinnard, R. Houlmann, P. Junod, B. Korzh, N. Kulesza, M. Legré, C. W. Lim, T. Lunghi, L. Monat, C. Portmann, M. Soucarros, R. T. Thew, P. Trinkler, G. Trolliet, F. Vannel, and H. Zbinden, New Journal of Physics **16** (2014), 10.1088/1367-2630/16/1/013047, arXiv:1309.2583.