Research Article | Vol. 25, No. 18 | 4 Sep 2017 | OPTICS EXPRESS 21275
Optics EXPRESS

Programmable dispersion on a photonic integrated circuit for classical and quantum applications

JELENA NOTAROS,[1] JACOB MOWER,[1] MIKKEL HEUCK,[1] COSMO LUPO,[2] NICHOLAS C. HARRIS,[1] GREGORY R. STEINBRECHER,[1] DARIUS BUNANDAR,[1] TOM BAEHR-JONES,[3] MICHAEL HOCHBERG,[3] SETH LLOYD,[2] AND DIRK ENGLUND[1,*]

[1]*Research Laboratory of Electronics, Massachusetts Institute of Technology, Cambridge, MA 02139, USA*
[2]*Department of Mechanical Engineering, Massachusetts Institute of Technology, Cambridge, MA 02139, USA*
[3]*Elenion Technologies, New York, NY 10016, USA*
[*]*englund@mit.edu*

Abstract: We demonstrate a large-scale tunable-coupling ring resonator array, suitable for high-dimensional classical and quantum transforms, in a CMOS-compatible silicon photonics platform. The device consists of a waveguide coupled to 15 ring-based dispersive elements with programmable linewidths and resonance frequencies. The ability to control both quality factor and frequency of each ring provides an unprecedented 30 degrees of freedom in dispersion control on a single spatial channel. This programmable dispersion control system has a range of applications, including mode-locked lasers, quantum key distribution, and photon-pair generation. We also propose a novel application enabled by this circuit – high-speed quantum communications using temporal-mode-based quantum data locking – and discuss the utility of the system for performing the high-dimensional unitary optical transformations necessary for a quantum data locking demonstration.

OCIS codes: (130.3120) Integrated optics devices; (130.2035) Dispersion compensation devices; (270.5565) Quantum communications.

References and links

1. H. A. Haus, J. G. Fujimoto, and E. P. Ippen, "Structures for additive pulse mode locking," J. Opt. Soc. Am. B **8**, 2068–2076 (1991).
2. C. Madsen, G. Lenz, A. Bruce, M. Cappuzzo, L. Gomez, and R. Scotti, "Integrated all-pass filters for tunable dispersion and dispersion slope compensation," IEEE Photon. Tech. Lett. **11**, 1623–1625 (1999).
3. N. Litchinitser, M. Sumetsky, and P. Westbrook, "Fiber-based tunable dispersion compensation," J. Opt. Fiber. Commun. Rep. **4**, 41–85 (2007).
4. A. Yariv, Y. Xu, R. K. Lee, and A. Scherer, "Coupled-resonator optical waveguide: a proposal and analysis," Opt. Lett. **24**, 711–713 (1999).
5. J. E. Heebner, P. Chak, S. Pereira, J. E. Sipe, and R. W. Boyd, "Distributed and localized feedback in microresonator sequences for linear and nonlinear optics," J. Opt. Soc. Am. B **21**, 1818–1832 (2004).
6. J. Mower, Z. Zhang, P. Desjardins, C. Lee, J. H. Shapiro, and D. Englund, "High-dimensional quantum key distribution using dispersive optics," Phys. Rev. A **87**, 062322 (2013).
7. D. Bunandar, Z. Zhang, J. H. Shapiro, and D. R. Englund, "Practical high-dimensional quantum key distribution with decoy states," Phys. Rev. A **91**, 022336 (2015).
8. C. Lupo, M. M. Wilde, and S. Lloyd, "Robust quantum data locking from phase modulation," Phys. Rev. A **90**, 022326 (2014).
9. M. Pant and D. Englund, "High-dimensional unitary transformations and boson sampling on temporal modes using dispersive optics," Phys. Rev. A **93**, 043803 (2016).
10. K. Inoue, E. Waks, and Y. Yamamoto, "Differential phase shift quantum key distribution," Phys. Rev. Lett. **89**, 037902 (2002).
11. T. Baehr-Jones, R. Ding, A. Ayazi, T. Pinguet, M. Streshinsky, N. Harris, J. Li, L. He, M. Gould, Y. Zhang, A. E.-J. Lim, T.-Y. Liow, S. H.-G. Teo, G.-Q. Lo, and M. Hochberg, "A 25 Gb/s silicon photonics platform," arXiv:1203.0767 (2012).

#290888 https://doi.org/10.1364/OE.25.021275
Journal © 2017 Received 31 May 2017; accepted 31 Jul 2017; published 23 Aug 2017

Optics EXPRESS

12. A. Yariv, "Critical coupling and its control in optical waveguide-ring resonator systems," IEEE Photon. Tech. Lett. **14**, 483–485 (2002).
13. H. Takahashi, R. Inohara, K. Nishimura, and M. Usami, "Expansion of bandwidth of tunable dispersion compensator based on ring resonators utilizing negative group delay," J. Lightwave Technol. **24**, 2276 (2006).
14. H. Shen, M. H. Khan, L. Fan, L. Zhao, Y. Xuan, J. Ouyang, L. T. Varghese, and M. Qi, "Eight-channel reconfigurable microring filters with tunable frequency, extinction ratio and bandwidth," Opt. Express **18**, 18067–18076 (2010).
15. W. M. Green, R. K. Lee, G. A. DeRose, A. Scherer, and A. Yariv, "Hybrid InGaAsP-InP Mach-Zehnder racetrack resonator for thermooptic switching and coupling control," Opt. Express **13**, 1651–1659 (2005).
16. C. M. Gentry, J. M. Shainline, M. T. Wade, M. J. Stevens, S. D. Dyer, X. Zeng, F. Pavanello, T. Gerrits, S. W. Nam, R. P. Mirin, and M. A. Popović, "Quantum-correlated photon pairs generated in a commercial 45 nm complementary metal-oxide semiconductor microelectronic chip," Optica **2**, 1065–1071 (2015).
17. D. P. DiVincenzo, M. Horodecki, D. W. Leung, J. A. Smolin, and B. M. Terhal, "Locking classical correlations in quantum states," Phys. Rev. Lett. **92**, 067902 (2004).
18. S. Lloyd, "Quantum enigma machines," arXiv:1307.0380 (2013).
19. A. Yariv, "Universal relations for coupling of optical power between microresonators and dielectric waveguides," Electron. Lett. **36**, 321–322 (2000).
20. N. C. Harris, Y. Ma, J. Mower, T. Baehr-Jones, D. Englund, M. Hochberg, and C. Galland, "Efficient, compact and low loss thermo-optic phase shifter in silicon," Opt. Express **22**, 10487–10493 (2014).
21. S. Ryu, Y. Horiuchi, and K. Mochizuki, "Novel chromatic dispersion measurement method over continuous gigahertz tuning range," J. Lightwave Technol. **7**, 1177–1180 (1989).
22. J. Notaros, F. Pavanello, M. T. Wade, C. Gentry, A. Atabaki, L. Alloatti, R. J. Ram, and M. Popovic, "Ultra-efficient CMOS fiber-to-chip grating couplers," in "Optical Fiber Communication Conference," OSA Technical Digest (Optical Society of America, 2016), paper M2I.5.
23. J. H. Schmid, P. Cheben, M. Rahim, S. Wang, D.-X. Xu, M. Vachon, S. Janz, J. Lapointe, Y. Painchaud, M.-J. Picard, M. Poulin, and M. Guy, "Subwavelength gratings for broadband and polarization independent fiber-chip coupling with -0.4 dB efficiency," in "Optical Fiber Communication Conference," OSA Technical Digest (Optical Society of America, 2016), paper M2I.4.
24. M. Powell, "Direct search algorithms for optimization calculations," Acta Numer. **7**, 287–336 (1998).
25. J. C. Mak, W. D. Sacher, T. Xue, J. C. Mikkelsen, Z. Yong, and J. K. Poon, "Automatic resonance alignment of high-order microring filters," IEEE J. Quant. Electron. **51**, 1–11 (2015).
26. H. Jayatilleka, K. Murray, M. Á. Guillén-Torres, M. Caverley, R. Hu, N. A. Jaeger, L. Chrostowski, and S. Shekhar, "Wavelength tuning and stabilization of microring-based filters using silicon in-resonator photoconductive heaters," Opt. Express **23**, 25084–25097 (2015).
27. J. C. Mak, A. Bois, and J. K. Poon, "Programmable multiring butterworth filters with automated resonance and coupling tuning," IEEE J. Sel. Topics Quantum Electron. **22**, 232–240 (2016).
28. P. Hayden, D. Leung, P. W. Shor, and A. Winter, "Randomizing quantum states: Constructions and applications," Commun. Math. Phys. **250**, 371–391 (2004).
29. O. Fawzi, P. Hayden, and P. Sen, "From low-distortion norm embeddings to explicit uncertainty relations and efficient information locking," J. ACM **60**, 44 (2013).
30. F. Dupuis, J. Florjanczyk, P. Hayden, and D. Leung, "The locking-decoding frontier for generic dynamics," Proc. R. Soc. A **469** 20130289 (2013).
31. S. Guha, P. Hayden, H. Krovi, S. Lloyd, C. Lupo, J. H. Shapiro, M. Takeoka, and M. M. Wilde, "Quantum enigma machines and the locking capacity of a quantum channel," Phys. Rev. X **4**, 011016 (2014).
32. C. Lupo and S. Lloyd, "Quantum-locked key distribution at nearly the classical capacity rate," Phys. Rev. Lett. **113**, 160502 (2014).
33. C. Lupo and S. Lloyd, "Quantum data locking for high-rate private communication," New J. Phys. **17**, 033022 (2015).
34. C. E. Shannon, "Communication theory of secrecy systems," Bell Syst. Tech. J. **28**, 656–715 (1949).
35. R. Adamczak, R. Latała, Z. Puchała, and K. Życzkowski, "Asymptotic entropic uncertainty relations," J. Math. Phys. **57**, 032204 (2016).
36. C. Lupo, "Quantum data locking for secure communication against an eavesdropper with time-limited storage," Entropy **17**, 3194–3204 (2015).
37. D. J. Lum, J. C. Howell, M. S. Allman, T. Gerrits, V. B. Verma, S. W. Nam, C. Lupo, and S. Lloyd, "Quantum enigma machine: Experimentally demonstrating quantum data locking," Phys. Rev. A **94**, 022315 (2016).
38. Y. Liu, Z. Cao, C. Wu, D. Fukuda, L. You, J. Zhong, T. Numata, S. Chen, W. Zhang, S.-C. Shi, C.-Y. Lu, Z. Wang, X. Ma, J. Fan, Q. Zhang, and J.-W. Pan, "Experimental quantum data locking," Phys. Rev. A **94**, 020301 (2016).
39. E. Timurdogan, C. M. Sorace-Agaskar, J. Sun, E. S. Hosseini, A. Biberman, and M. R. Watts, "An ultralow power athermal silicon modulator," Nat. Commun. **5** (2014).
40. Q. Xu, B. Schmidt, S. Pradhan, and M. Lipson, "Micrometre-scale silicon electro-optic modulator," Nature **435**, 325–327 (2005).
41. M. R. Watts, J. Sun, C. DeRose, D. C. Trotter, R. W. Young, and G. N. Nielson, "Adiabatic thermo-optic mach–zehnder switch," Opt. Lett. **38**, 733–735 (2013).

Optics EXPRESS

1. Introduction and motivation

Control of dispersion is of central importance in many optical applications ranging from compensation for fiber-induced dispersion in communications systems to tunable group-velocity dispersion for mode locking of laser sources [1, 2]. Historically, these problems have been addressed using devices such as chirped fiber gratings [3], coupled resonator optical waveguides (CROWs) [4], or side-coupled integrated spaced sequences of resonators (SCISSORs) [5]. However, as interest turns towards dispersion-based quantum applications [6–10], dispersion control with a large number of tunable parameters is needed to enable a large set of basis states. For these applications, prior solutions do not provide the tunability, speeds, and scalability necessary for practical demonstrations. Integrated silicon photonics, capable of controlling many modes in a phase-stable way, presents one possible approach to large-scale dispersion control.

In this paper, we leverage a modern silicon foundry platform [11] to enable large-scale dispersion control using an on-chip tunable-coupling ring resonator array. By integrating each ring into a Mach-Zehnder interferometer (MZI) coupling geometry, it is possible to independently control the quality factor and resonance frequencies of each dispersive resonator, as demonstrated in a variety platforms [2, 12–15]. By cascading 15 of these tunable-coupling rings, we enable a system with 30 individually-controllable degrees of freedom with >10 bits of resolution each.

This large-scale tunable-coupling ring array has many benefits in both classical and quantum applications. The array allows for reconfigurable dispersion control in a range of classical applications, including mode-locked lasers for frequency comb generation and higher-order optical dispersion cancellation for communications and sensing [1, 2]. In the area of quantum information processing, benefits of the system include tunable dispersion for temporal-mode high-dimensional quantum key distribution [6, 7] and pulse-shaping of photon pairs generated by spontaneous four-wave mixing [16]. In this paper, we highlight one specific application of the tunable-coupling ring array: high-speed one-way quantum-secure communications using a quantum enigma machine [17, 18]. Specifically, we propose a novel protocol based on phase-encoded quantum data locking for the first chip-based quantum enigma machines and discuss application of the programmable dispersion system for enabling the protocol in a phase-stable, scalable, and integrated way. The results indicate utility of the programmable dispersion circuit for future demonstrations of photonic quantum data locking.

2. Tunable-coupling resonator array theory and simulation

A ring resonator coupled to a photonic waveguide, as shown in Fig. 1(a), induces a frequency-dependent phase shift on the transmitted mode of the waveguide across the frequency linewidth of the ring. For standard rings coupled to a single bus waveguide through a directional coupler, this resonance is tuned using a phase shifting device such as a thermo-optic modulator. However, the ring's frequency linewidth is fixed. By introducing an integrated interferometer with an additional phase shift, Θ, as shown in Fig. 1(b), it is possible to also dynamically control the coupling rate between this modified ring and the waveguide [2, 12].

From coupled mode theory, it is possible to derive the transmission through a single tunable-coupling ring. Assuming waveguide modes A_1 and B_1 and ring modes A_2 and B_2, as shown in

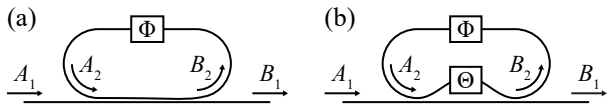

Fig. 1. Schematic of (a) a ring with tunable resonance and (b) a ring with tunable coupling and resonance (a tunable-coupling ring). The resonant frequency is set using phase Φ and the coupling is set using phase Θ.

Optics EXPRESS

Fig. 1, the coupled equation is given as

$$\begin{bmatrix} B_1 \\ B_2 \end{bmatrix} = M \begin{bmatrix} A_1 \\ A_2 \end{bmatrix} \tag{1}$$

where the transfer matrix, M, depends on the coupling between the ring resonator and the bus waveguide. Assuming a standard ring with a directional coupler shown in Fig. 1(a), the matrix takes the form [19]

$$M_{\text{coupler}} = \frac{1}{\sqrt{2}} \begin{bmatrix} \kappa & i\sqrt{1-\kappa^2} \\ i\sqrt{1-\kappa^2} & \kappa \end{bmatrix} \tag{2}$$

where the coupling coefficient, κ, is largely set during fabrication. However, if a tunable Mach-Zehnder interferometer (MZI) is used to couple the ring to the bus waveguide, the transfer matrix takes the form

$$M_{\text{MZI}} = e^{i(\Theta/2+\pi/2)} \begin{bmatrix} \sin(\Theta/2) & \cos(\Theta/2) \\ \cos(\Theta/2) & -\sin(\Theta/2) \end{bmatrix} \tag{3}$$

where Θ is the phase shift induced by the MZI. In addition to the coupled equation, the feedback condition for the ring is given as

$$A_2 = \alpha e^{i(\beta(\omega)L+\Phi)} B_2 \tag{4}$$

where α is the intrinsic cavity loss rate per circulation, $\beta(\omega) = n_{\text{eff}}\omega/c_0$ is the frequency-dependent propagation constant, ω is the angular frequency, c_0 is the speed of light in vacuum, n_{eff} is the effective refractive index, L is the ring length, and Φ is the phase shift induced by the resonance phase setting. Using this feedback equation and the transfer matrix in Eq. (3), the transmission through the tunable-coupling ring is derived to be [12]:

$$T(\omega) = \frac{B_1}{A_1} = \frac{1 - e^{i\Theta} + 2e^{i(\beta(\omega)L+\Phi+\Theta)}\alpha}{2 - e^{i(\beta(\omega)L+\Phi)}\alpha + e^{i(\beta(\omega)L+\Phi+\Theta)}\alpha}. \tag{5}$$

Figure 2 plots the power transmission, $|T(\omega)|^2$, and group delay, $\tau(\omega) = -d\angle T(\omega)/d\omega$ where $\angle T(\omega)$ is the transmission phase angle, as a function of wavelength for varying resonance and

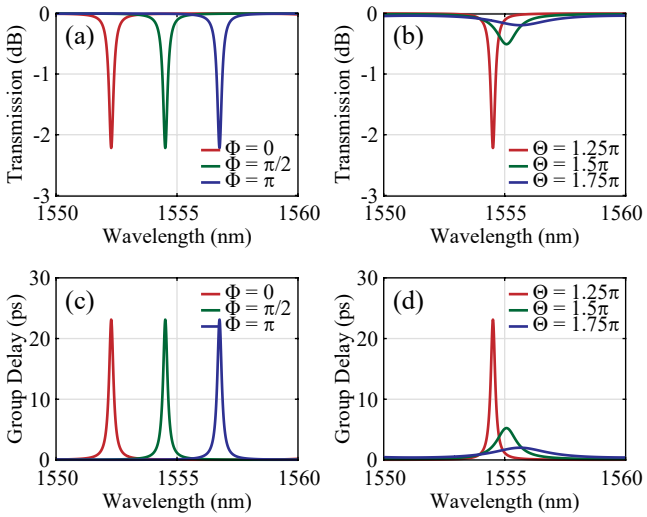

Fig. 2. Simulated transmission and group delay as a function of wavelength for varying (a,c) resonance phase setting, Φ, and (b,d) coupling phase setting, Θ, for a single tunable-coupling ring with $\alpha = 0.99$, $L = 100\mu$m, and $n_{\text{eff}} = 2.7$.

Optics EXPRESS

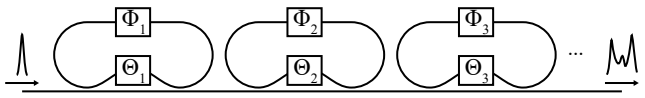

Fig. 3. Schematic of the tunable-coupling ring array (TCRA) with three rings shown. The ring resonant frequencies are set using phases Φ_j and the couplings are set using phases Θ_j.

coupling phase settings. Group delay is chosen as a performance metric since it is the quantity of interest in many applications, including dispersive-optics quantum key distribution and quantum data locking, and is directly related to phase by the derivate with respect to frequency. As shown in Fig. 2, varying Φ shifts the resonance wavelength while varying Θ adjusts the coupling of the ring in addition to inducing a slight resonance shift, as expected.

When multiple tunable-coupling rings are cascaded together in series to form a tunable-coupling ring array (TCRA) (see Fig. 3) [2, 14], the transfer function of the full device with N rings is the product of the functions of the individual rings:

$$T_N(\omega) = \prod_{j=1}^{n} T_j(\omega) = \prod_{j=1}^{n} \frac{1 - e^{i\Theta_j} + 2e^{i(\beta(\omega)L+\Phi_j+\Theta_j)}\alpha_j}{2 - e^{i(\beta(\omega)L+\Phi_j)}\alpha_j + e^{i(\beta(\omega)L+\Phi_j+\Theta_j)}\alpha_j} \tag{6}$$

where j is the index of each tunable-coupling ring in the array and α_j, Θ_j, and Φ_j are the intrinsic cavity loss rates, coupling MZI phase shifts, and resonance phase shifts, respectively, of each ring.

To achieve a target frequency-dependent dispersion function given by the transfer function, $T_{\text{target}}(\omega)$, we must find the parameters of the TCRA system to suitably approximate T_{target}. We do this by setting the Θ_j and Φ_j phase shifts (a total of $2N$ parameters) using a standard MATLAB interior-point nonlinear optimization procedure for minimizing the mean squared error. As an example, we optimize the phase settings for a TCRA with 15 tunable-coupling rings

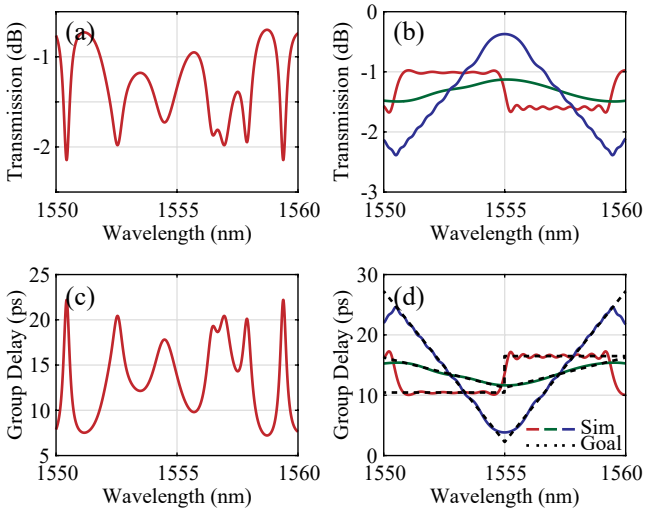

Fig. 4. Simulated example transmissions and group delays for a 15-ring tunable-coupling ring array device with $\alpha = 0.99$, $L = 100\mu$m, and $n_{\text{eff}} = 2.7$. (a,c) Arbitrary device spectrum with phase settings set to random values between 0 and 2π. (b,d) Example optimization of this device for three goal group delay functions. The goal group delays are shown as dashed lines while the optimized simulations are shown as solid lines.

Optics EXPRESS

for a variety of square-wave and triangle-wave goal group delay functions. As shown in Fig. 4, the single TCRA simulated device is able to closely match various desired group delays and can create a large set of phase transformations suitable for high-dimensional quantum applications. The bandwidth of the system is limited by the free spectral range of the largest ring in the array and the bandwidth-utilization ratio [13]. Additionally, when the number of rings in the system is increased, the number of discernible phase settings and corresponding transformations grows.

3. Tunable-coupling resonator array experimental demonstration

Experimentally implementing a large-scale tunable-dispersion system, such as the proposed TCRA, becomes extremely challenging for bulk-optics approaches as it requires many phase-stable interferometers. Photonic integrated circuits offer a solution but require careful design to allow such a large number of parameters to be individually controlled with precision and minimal cross-talk. In this work, we leverage a modern silicon photonics foundry coupled with driving electronics to demonstrate the proposed TCRA system.

Specifically, we fabricate a 15-ring TCRA system in a silicon-on-insulator (SOI) process in collaboration with the OpSIS foundry [11]. The device is fabricated on a 200 mm SOI wafer with 220 nm device layer thickness and 2 μm buried oxide thickness. 248 nm photolithography defines the resist patterns, based around 500 nm wide waveguides. Top oxide is deposited on the chip, aluminum vias are defined through the oxide to access active devices on the device layers, and aluminum contact pads are written on the top oxide for contact to wire bonds or probes. An optical micrograph of the fabricated device is shown in Fig. 5(b).

Each ring contains three thermo-optic modulator heaters with a 130 kHz modulation bandwidth and 0.23 dB insertion loss [20], as shown in Figs. 5(a) and 5(c) – one to actively set the ring resonant frequency, one to actively control coupling, and the last to passively balance the loss of the coupling heater. The voltage across each of the 30 active heaters is dynamically controlled using a custom-designed electrical driver which is wire bonded to the chip using a printed

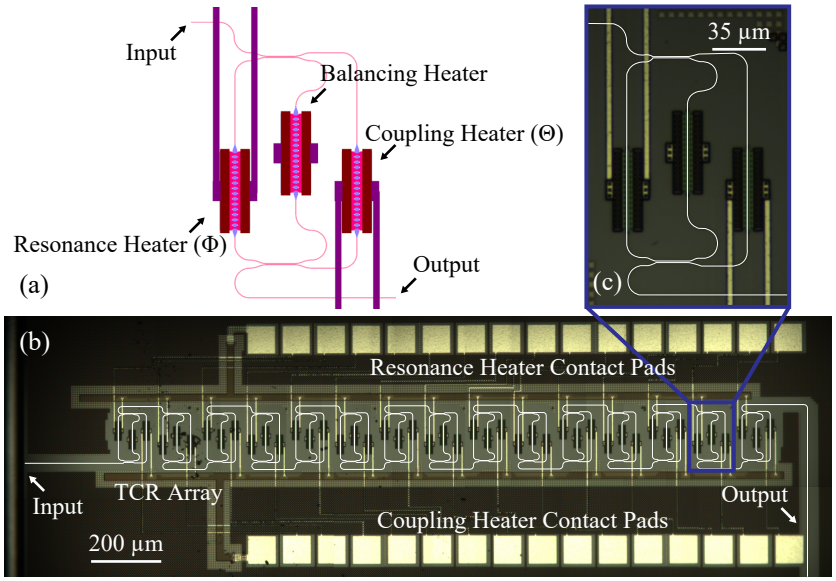

Fig. 5. (a) Layout of a single tunable-coupling ring. Optical micrographs of (b) the full fabricated 15-ring tunable-coupling ring array device and (c) a single tunable-coupling ring within the 15-ring array (device waveguides are traced in white on the micrographs for clarity).

Optics EXPRESS

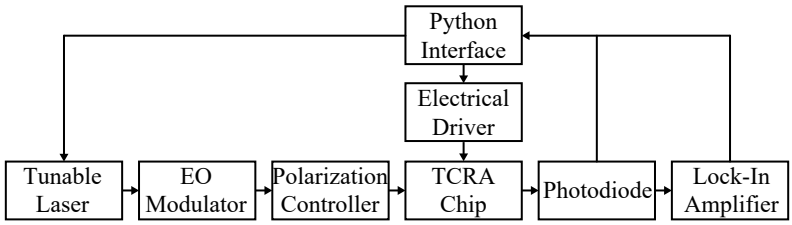

Fig. 6. Block diagram illustrating the experimental setup used to characterize the tunable-coupling ring array device. A modulated laser source is coupled onto the chip and the output signal is read using an off-chip photodiode. A lock-in amplifier is used to convert the photodiode signal to a phase measurement [21]. A Python interface reads the lock-in amplifier's phase measurement and photodiode's intensity output, controls an electrical driver circuit, and sweeps the tunable laser.

circuit board (PCB) and set through a Python user interface. The chip is optically interfaced by coupling two ultra-high-numerical-aperture (UHNA) fibers to the input and output waveguides. To measure the group delay through the structure, we implement a heterodyne modulation phase-shift technique using an optical modulator and lock-in amplifier [21]. A diagram illustrating the experimental setup is shown in Fig. 6.

Figure 7 shows a passive spectrum of the TCRA device. The device exhibits many resonance dips with varying resonance frequencies and quality factors characteristic of a multi-ring untuned device. The spectrum indicates a working bandwidth of approximately 1.5 nm which is expected given the design ring length of ~430 μm. An imperfect mode matching to the fiber resulted in a relatively high fiber-to-waveguide coupling loss of ~8 dB; however, this loss can be reduced to well below 0.5 dB through optimized edge or vertical grating couplers [22, 23].

To characterize the functionality of the system, we individually vary the resonance and coupling heater voltages for one of the tunable-coupling rings in the array, as shown in Fig. 8. As predicted in simulation, by increasing the voltage across the resonance heater, the ring's transmission dip shifts to longer wavelengths (Figs. 8(a) and 8(c)) while increasing the coupling heater voltage results in decreased coupling of the ring and a lower quality factor in addition to a slight resonance shift (Figs. 8(b) and (d)). By optimizing these coupling settings, we measure quality factors over 150, 000 for each ring in the system. These maximum quality factor settings result in a maximum of ~20 dB of on-chip loss per ring.

Using a Python interface, we optimize the 30 heater voltages on the tunable-coupling ring array device in unison so that the device applies a desired frequency-dependent group delay to the output signal. To perform this optimization, we use a constrained optimization by linear approximation (COBYLA) method (available in the SciPy open-source Python package) [24]. The optimization takes as input a goal frequency-dependent group delay function. Then, within

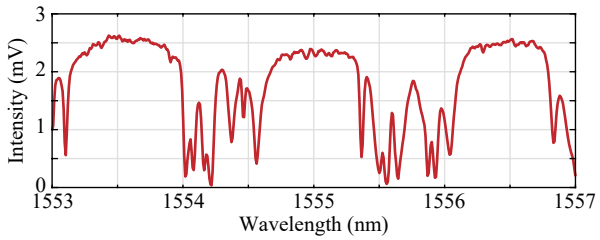

Fig. 7. Passive spectrum of the 15-ring tunable-coupling ring array device.

Optics EXPRESS

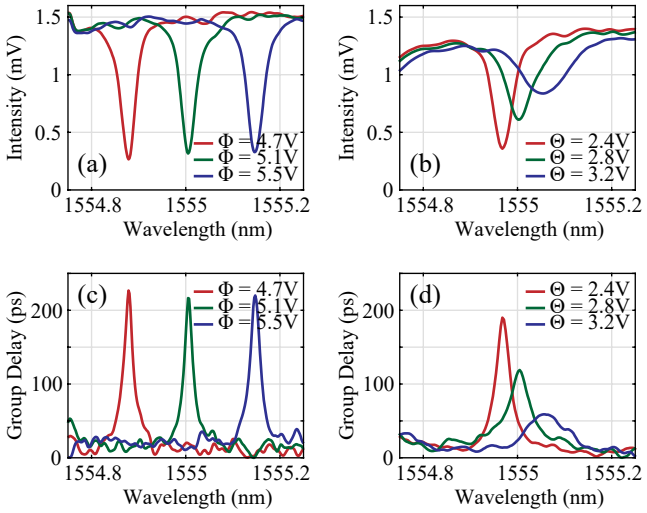

Fig. 8. Active tuning of a single ring in the tunable-coupling ring array device. Measured intensity and group delay as a function of wavelength for varying (a,c) resonance phase shifter voltage, Φ, and (b,d) coupling phase shifter voltage, Θ.

each optimization step, the program reads the current group delay by sweeping the laser and reading the lock-in amplifier signal, compares this read signal to the goal group delay spectrum, and sets the 30 heater voltages based on the COBYLA method. The optimization is complete once the goal group delay has been reached or a maximum number of user-defined optimization steps has been performed. Any thermal crosstalk resulting from varying the heaters is compensated as a part of the optimization procedure and can be even further reduced by introducing a thermoelectric cooler element for temperature stability. (Automation of high-order ring filter tuning, either through similar multi-dimensional optimization algorithms [25] or using on-chip sensors such as in-resonator photoconductive heaters [26] and reference ports [27], has been explored.)

As an example, we program the device to demonstrate linear group delay. Figure 9 shows the goal and measured group delay spectra at various stages. Initially, before the heater voltages are set, the wavelength range of interest is within the passband of the device and no characteristic group delay is seen. As we optimize the device, the group delay spectra begins to resemble

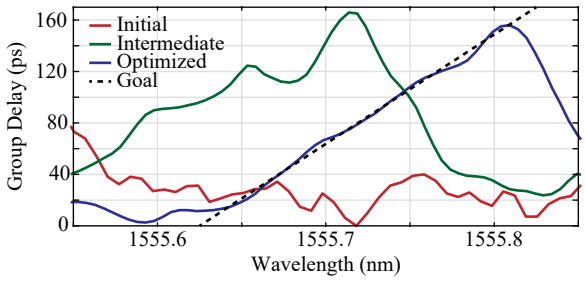

Fig. 9. Optimization of the 15-ring tunable-coupling ring array device for an example goal group delay function (shown as a dashed line). The measured group delay spectra is shown in its initial state before the optimization has begun (solid red line), at an intermediate point within the optimization (solid green line), and in the final optimized state (solid blue line).

Optics EXPRESS

a linear function, as shown by the solid green intermediate line in Fig. 9. Finally, when the optimization is complete, the solid blue optimized line closely follows the goal group delay function.

Using the optimization procedure, we can program a large-scale set of independent group delay spectra and, consequently, determine their corresponding heater voltage settings for a variety of high-dimensional classical and quantum applications.

4. Application to quantum data locking and the quantum enigma machine

We now consider the utility of the demonstrated programmable dispersion system for efficient and quantum-secure communications through quantum data locking [17, 18, 28–30]. In particular, we propose a new temporal-mode-based "quantum enigma machine" protocol and discuss how the programmable circuit shows promise in enabling the protocol on-chip in a phase-stable, scalable, and fully-integrated way.

The "quantum enigma machine" [18] is a quantum optical cipher that utilizes quantum data locking to enable a relatively small key to encrypt and decrypt a much larger amount of data at the channel's transmitter and receiver, respectively. The protocol allows for faster and more efficient quantum-secure communications under practical conditions – channels secure to eavesdropping under noisy and lossy conditions [18, 31–33].

It follows from classical information theory that secure encryption of n bits of classical information requires at least n classical bits of secret key [34]. On the other hand, quantum data locking [17] enables a key of length $\ll n$ bits shared a priori and secretly between Alice, the transmitter, and Bob, the receiver, to securely encrypt a substantially larger amount of data on the order of n bits (see Fig. 10) [28–30, 35]. As shown in [32, 33, 36], quantum data locking guarantees composable security under the condition that the eavesdropper is restricted to either a finite-coherence-time quantum memory or no quantum memory at all. Due to these less stringent secret key requirements and security under lossy and noisy conditions, the quantum enigma machine is an attractive approach for high-speed secure quantum communications.

To realize such a system, a recent protocol proposed coherently splitting a photon over multiple modes (e.g. temporal or spatial modes), encoding the photon by applying independent, random phase shifts to each mode, and decoding at the receiver using the corresponding inverse transformation [8]. Compared to other proposed data locking methods that require Haar-distibuted random unitaries [28], single unitaries with keys limited to a subset of qubits [30], or universal quantum computers [29], this scheme enables quantum data locking using standard linear optics, which greatly simplifies its implementation.

Although recent demonstrations have realized quantum data locking using bulk optical components [37, 38], scaling to larger mode numbers (i.e. larger dimensionality) requires a degree of phase stability and device complexity that is difficult to realize using bulk optics. As such, our

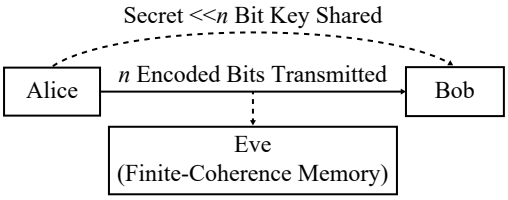

Fig. 10. Schematic of a quantum enigma machine protocol. A relatively small key of $\ll n$ bits is shared between Alice, the transmitter, and Bob, the receiver, and used to encode, and decode, the n bit message. The protocol guarantees composable security against an eavesdropper, Eve, with either a finite-coherence-time memory or no quantum memory at all.

Optics EXPRESS

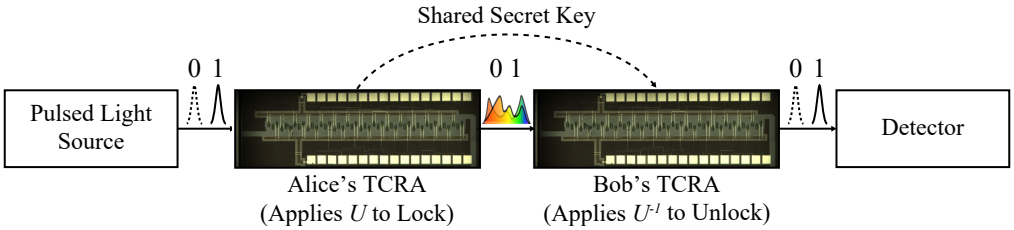

Fig. 11. Proposed quantum enigma machine protocol using the tunable-coupling ring array device. Photons are prepared in a time domain basis using a pulsed light source, locked using Alice's TCRA, transmitted over a public channel, and unlocked using Bob's TCRA. Alice's and Bob's TCRA settings for each transmission are determined using a secret pre-shared key.

chip-integrated tunable coupling ring array implementation is an attractive alternative due to the excellent phase stability, scalability, and integration with electronics natively provided by mature silicon platforms [11].

Using the tunable-coupling ring array, a quantum enigma machine can be implemented based on a modified temporal-mode phase-encoded quantum data locking protocol, as shown in Fig. 11. Suppose Alice, the transmitter, and Bob, the receiver, want to transmit n bits of information securely. In this protocol, Alice encodes the bits in photons coherently split over d time bins in a time domain basis [6] such that each photon encodes $\log_2(d)$ bits of information and, consequently, only $p = n/\log_2(d)$ photons are needed to transmit the n bit message.

To lock the information, Alice scrambles each photon using predetermined heater settings to apply an independent group-delay transformation, U, to each photon. On the receiving device, Bob applies the inverse group-delay transformation, U^{-1}, to undo the locking and recover the information. To lock and transmit the entire message, a total of p transformation settings (and their unlocking counterparts) are needed.

The order that these p transformations are applied is picked from a list of k possible sequences where k has been proven to be $O(2^p)$ for guaranteed composable security [32,33,36]. Therefore, Alice and Bob only need to secretly and a priori share a key of length p bits to know which one of the k sequences to pick and, consequently, which sequence of transformations (or inverse transformations) to apply.

In summary, using this quantum data locking protocol, only $p = n/\log_2(d)$ bits of secret key are needed to securely transmit n bits of information. If d is sufficiently large, the number of necessary secret key bits becomes much smaller than the number of securely transmitted message bits. By integrating the quantum enigma machine transceivers on chip to enable these high-dimensional unitary transformations, the tunable coupling ring array device shows promise for enabling highly-efficient quantum-secure communications.

Although the intrinsic loss of the ring resonators in the photonic circuit causes some loss in the overall system, any loss inside Alice's transmitter can be compensated by increasing the power of the coherent pump (as long as the mean-photon number per pulse exiting her setup is below unity) while the loss in Bob's receiver chip can be factored into the overall channel loss and accounted for in the quantum enigma machine protocol [18,32].

For practical and high-data-rate demonstrations of the full protocol, the insertion loss of Bob's photonic components should be reduced and high-speed phase shifters should be implemented. Specifically, the fiber-to-chip coupling losses could be dramatically reduced to below 0.5 dB using optimized edge or vertical grating couplers [22, 23]. Furthermore, the current on-chip thermo-optic phase shifters with 130 kHz modulation speeds [20] could be replaced with free-carrier injection or depletion based devices [39, 40] to enable high-speed modulation of the

Optics EXPRESS

encoding/decoding transformations and, consequently, higher data rates.

5. Discussion and applications

In this paper, we have proposed and experimentally demonstrated a large-scale array of 15 tunable-coupling rings in a CMOS-compatible silicon photonics platform. The array uses a Mach-Zehnder interferometer architecture to enable independent control of the resonance frequency and coupling of each ring within the system using on-chip thermo-optic phase shifters. Through dynamic control of these 30 voltage parameters, we have shown tunable frequency-dependent group delay suitable for a variety of classical and quantum applications. The successful realization of such a system represents an important step towards phase-stable and practical chip-based quantum data locking, though future work is needed to reduce insertion losses and increase the switching rate between transformations. Future improvements to the device include incorporating lower-loss components such as adiabatic phase shifters [41] and grating couplers [22] to increase overall system efficiency and replacing the thermo-optic heaters with faster electro-optic modulators for high-speed operation [39, 40].

The demonstrated tunable-coupling ring array promises new applications in a range of other quantum optics applications. For example, quantum key distribution using dispersive optics [6, 7], currently implemented using off-chip dispersive elements, would benefit from the on-chip dynamic dispersion control enabled by this device. Furthermore, boson sampling experiments using temporal encoding [9] require time-dependent dispersion that could be implemented on chip with the tunable-coupling ring array. Finally, the device could enable fabrication-tolerant notch filters for precise bandwidth matching and laser line filtering for single photon-pair generation by spontaneous four-wave mixing [16].

Funding

Air Force Office of Scientific Research Multidisciplinary University Research Initiative (AFOSR MURI) for Optimal Measurements for Scalable Quantum Technologies (Grant No. FA9550-14-1-0052); Defense Advanced Research Projects Agency (DARPA) QUINESS program (Grant No. W31P4Q-12-1-0019); National Science Foundation Graduate Research Fellowship (Grant No. 1122374); Danish Research Council (Grant No. DFF - 1325-00144); Air Force Office of Scientific Research OpSIS (Grant No. FA9550-10-1-0439).