Integrated silicon photonics as a platform for quantum cryptographic tasks

Daniel Hutama[1] and Adrian Chan[1]

***Abstract*— Contemporary classical cryptographic protocols exhibit vulnerabilities to attacks from emerging quantum technologies. Most notably, a quantum device capable of performing Shor's algorithm can efficiently defeat the commonly used RSA asymmetric key distribution protocol. Here, we describe how integrated silicon photonics provides a platform for such a quantum device. In addition, we discuss how silicon photonics can provide a provably secure alternative to vulnerable communication protocols by facilitating scalable quantum key distribution (QKD). In particular, we discuss an implementation of the BB84 QKD protocol in integrated silicon photonics. The goal of this paper is to highlight how silicon photonics provides a platform to both attack and resolve weaknesses in classical information security.**

I. Introduction

Integer factorization is a problem that has been studied by mathematicians for centuries, but has yet to see an efficient classical solution. The apparent intractability of the factorization problem has become the cornerstone of several cryptosystems, such as the widely used RSA encryption scheme [1]. Several modern internet security protocols, such as Secure Shell, SSL/TLS, S/MIME, and OpenPGP, rely on RSA encryption, making RSA one of the most economically important cryptographic systems.

At its core, the RSA scheme is an asymmetric encryption protocol, in which a message's receiver generates a public key/private key pair. The recipient then broadcasts the public key and safeguards the private key. Any sender can use the broadcasted public key to encrypt a message, while only the receiver can decrypt messages using the private key. The primary vulnerability in the RSA scheme lies in the public key, which obfuscates the private key behind the integer factorization problem. If integer factorization can be performed efficiently, the private key can be obtained from the public key and used to decrypt any past and future messages encrypted with the public key.

In 1994, Peter Shor published a quantum algorithm capable of factoring an n-bit integer N in a number of steps polynomial in the input size (i.e. the bit-length n) [2]. In particular, Shor's algorithm factors an n-bit integer with a time complexity of $\mathcal{O}(n^2(\log n)(\log(\log n)))$, while the most efficient known classical factoring algorithm runs with a time complexity of $\mathcal{O}(\exp\big((\frac{64}{9})^{1/3}n^{1/3}(\log n)^{2/3}\big)$ [3]. The realization of a quantum computer running Shor's algorithm (with a sufficient number of qubits capable of maintaining quantum coherence and performing error correction) may one day make the large-N factorization problem tractable, thus breaking the effectiveness of RSA.

In this paper, we discuss recent developments in silicon photonics related to modern encryption. We first discuss how silicon photonics provides a platform to attack RSA encryption via an implementation of Shor's algorithm. Following this, we discuss how silicon photonics facilitates a quantum-secure encryption alternative. Specifically, we discuss a recent implementation of the BB84 quantum key distribution (QKD) protocol, which is used to establish symmetric (shared) private keys between the sender and receiver for use in unbreakable one-time pads.

II. Shor's Algorithm

Instead of utilizing a brute-force approach, Shor's algorithm considers a related number-theoretic problem. In particular, Shor's approach is to compute r, the period of a modulo N, where a is a randomly chosen seed value between 1 and N. The factorization of N can be accomplished via period-finding in five (high level) steps: (1) Pick a random seed value a, with $1 < a < N$. (2) Compute the greatest common divisor of a and N via the Euclidean algorithm. If $\gcd(a, N) \neq 1$, we have found a non-trivial factor of N. If $\gcd(a, N) = 1$, continue. (3) Compute r, the period of $a \pmod N$, i.e. find r, such that $a^r \equiv 1 \pmod N$. (4) Check that r is even and that $a^{r/2} \not\equiv \pm 1 \pmod N$. If this condition is violated, return to step 1. Otherwise, continue. (5) The factorization of $N = pq$ is achieved by computing $p = \gcd(a^{r/2} - 1, N)$ and $q = \gcd(a^{r/2} + 1, N)$ [2].

The focus of Shor's algorithm is on step (3), which is made efficient on a quantum computer [2], [4]. In short, Shor's algorithm begins with a quantum computer initialized with two entangled quantum registers. The qubits in the first register are placed in a superposition state using Hadamard gates. Following this, modular exponentiation is applied on the second register, conditional on the states of the qubits in the first register. A Fourier transform is applied to the first register to encode the function's period in a measurement probability amplitude. Finally a measurement of the first register yields classical data, from which we can obtain the function's period using the classical method of continued fractions [2].

A. Silicon Photonics

While Shor's algorithm is proven to be able to factor an integer exponentially faster than classical algorithms, it has yet to be implemented on a scale large enough to be a threat to modern encryption. The most efficient known quantum

[1]The Photonic Systems Group, Department of Electrical and Computer Engineering, McGill University, 3480 University St. room 753, Montreal, Quebec H3A 2A7

circuit description of Shor's algorithm for an arbitrary integer of bit-size n requires a quantum circuit of size $2n+2$ qubits [4]. At time of writing, the most powerful universal quantum computers can manipulate up to 54 qubits, much less than is required to break 1024-bit RSA [5]. However, compiled versions (i.e. one in which the factors are already known) of Shor's algorithm have been demonstrated in experiments with liquid-state NMR and bulk optical logic gates [6]. Such compiled versions can operate with fewer than the $2n+2$ qubits required for arbitrary integer factorization.

Politi *et al.* demonstrate a compiled device that is able to factor $N = 15$ $(n = 4)$ into its prime factors, $p = 3$ and $q = 5$, using five photonic qubits. In their compiled version, they choose $a = 2$. This specific choice of compilation reduces the total number of qubits needed, and also eliminates the need to impliment a quantum Fourier transform [7].

The fabricated device is a silicon photonic circuit in which four primary single photons and one auxiliary photon are generated via spontaneous parametric down-conversion (SPDC) and simultaneously injected into the circuit via edge-coupling. The primary photons are initialized in the path state $|0\rangle_{x1}|0\rangle_{x2}|0\rangle_{f1}|1\rangle_{f2}$ where the bit value is determined by the input port, as shown in Figure 1b. Qubits are then placed in a superposition of all possible four-bit states via Hadamard gates, which are implemented with half-reflectivity directional couplers. The compiled function is then implemented with two independent, non-deterministic controlled phase (CZ) gates, which are formed by a network of three 1/3 directional couplers. In particular, the function imparts a controlled phase shift on the qubit in the f_i register, dependent on the corresponding qubit in the x_i register being in the $|1\rangle$ state.

As a result of the quantum nature of the single photons passing through the circuit, the output of the device is probabilistic and determined by the specific photon path on each trial. Results in Figure 1c, show the measurement results of the first (x_i) register, where the four binary outcomes are 000_2, 010_2, 100_2, and 110_2, corresponding to the decimal values of 0, 2, 4, and 6, respectively. The first result, 000_2, is an expected failure inherent to Shor's algorithm. The third result 100_2 yields trivial factors 1 and 15, while the second and fourth results yield $r = 4$ via the method of continued fractions [7]. The expected results of $p = \gcd(2^{4/2}-1, 15) = 3$ and $q = \gcd(2^{4/2}+1, 15) = 5$ can then be classically computed via the Euclidean algorithm.

While Shor's algorithm in silicon photonics has been limited to compiled versions, such experiments show the potential it has in the field of quantum computing. As the field evolves with other quantum technologies, it will become increasingly important to develop encryption protocols that are resistant to quantum attacks. We show in the next section how silicon photonics is uniquely positioned to facilitate the widespread adoption of a quantum secure protocol.

III. Quantum Key Distribution

Silicon photonics is a promising platform for quantum key distribution (QKD), since bit states can easily be encoded in several different ways. For instance, binary 1s and 0s can be implemented via photon path, polarization, or incident power to name a few. Furthermore, by utilizing the widely available and mature CMOS fabrication technologies, silicon photonics can facilitate the widespread distribution of quantum communication devices. In this section, we discuss an implementation of QKD in silicon photonics. Following this, we discuss recent developments regarding single photon generation and detection in silicon photonics for use in quantum information technologies.

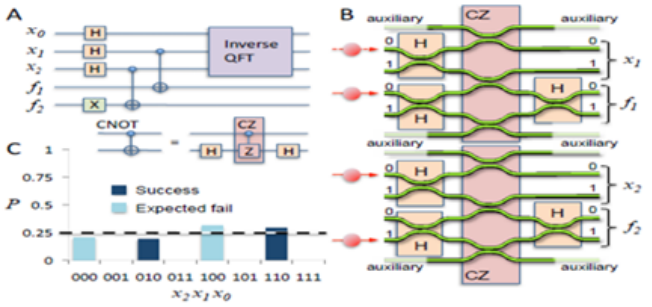

Fig. 1. **a**, Quantum circuit. **b**, Schematic of waveguide on the chip device. Qubits in the first register are denoted x_i, while qubits in the second register are denoted f_i. **c**, Results of measurement on the first register after applying the function. [8]

A. BB84

The BB84 QKD protocol is a provably secure, symmetric key distribution protocol [9], [10]. In the BB84 scheme, two parties, Alice and Bob, wish to establish a shared private key to securely encrypt subsequent transmissions. To establish the shared key, Alice transmits a sequence of bits, which are randomly prepared in one of two polarization bases. For instance, we can define the $+$ basis in which binary $|1_+\rangle$ corresponds to vertical polarization $|\updownarrow\rangle$ and binary $|0_+\rangle$ corresponds to horizontal polarization $|\leftrightarrow\rangle$. In the $\times$ basis, binary $|1_\times\rangle$ corresponds to $135°$ polarization $|\nwarrow\!\!\searrow\rangle$, while binary $|0_\times\rangle$ corresponds to $45°$ polarization $|\swarrow\!\!\nearrow\rangle$. Bob then measures the received bit in one of the two polarization bases. If the measurement basis matches the generation basis, Bob will measure the correct bit value (e.g. $||\langle 1_+|1_+\rangle||^2 = 1$, $||\langle 0_+|1_+\rangle||^2 = 0$). However, if the measurement basis is incorrect, Bob will measure the correct bit with 50% probability (e.g. $||\langle 1_\times|1_+\rangle||^2 = ||\langle 0_\times|1_+\rangle||^2 = 0.5$). Once Bob publicly announces that he has received Alice's transmission, Alice communicates her choice of bases to Bob. Both Alice and Bob discard the bits in which the bases do not match. The remaining bits form the shared secret key.

The security of the protocol comes from the no-cloning theorem, which prevents an eavesdropper, Eve, from covertly tapping the channel without disturbing the states of Alice's transmitted bits [10]. If Eve were to attempt to intercept and re-transmit the secret key, her measurements would collapse the states of the bits transmitted by Alice. The discrepancy can then be detected statistically during the resolution phase between Alice and Bob. If this discrepancy is detected, Alice and Bob can simply restart the protocol.

B. BB84 in Silicon Photonics.

Bunandar *et al.* demonstrate a QKD encoder in silicon photonics based on the BB84 protocol [11]. The device consists of a 10 Gbps Mach-Zehnder modulator (MZM) with polarization-splitting grating couplers (PSGCs), shown in Figure 2. The PSGCs are used to convert the orthogonal components of the elliptically polarized field in the input fiber into separate TE mode paths on the PIC and vice-versa [12]. Within the PIC, the relative phases between the two paths are controlled using the MZM. The phase modulators are based on depletion-mode free-carrier dispersion implemented with a doped p-i-n junction. The overlap of the free-carriers and optical mode results in free-carrier refraction. Phase modulation is achieved by controlling the refraction via gigahertz RF signals. The photon polarization in the output fiber is controlled by the relative phase shift between the top and bottom paths imparted by the MZM.

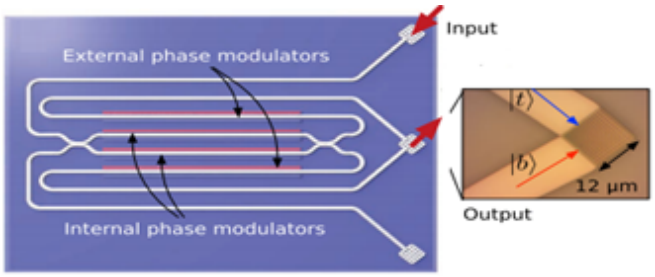

Fig. 2. From [11]. Silicon photonic path-to-polarization encoder for the BB84 protocol.

The device is initialized to produce the state $(|t\rangle+|b\rangle)/\sqrt{2}$, which is set as the $|0_+\rangle$ state. The MZM is then adjusted to generate $(|t\rangle + e^{i\phi}|b\rangle)/\sqrt{2}$, where ϕ is the phase shift applied by using RF signals of differing voltages. All four required states for the BB84 protocol can be generated by applying phase shifts of $\phi = 0, \pi/2, \pi$, and $3\pi/2$, as shown in Table I. Following transmission over a 43 km fiber, the polarization states are measured using a polarization beam splitter followed by InGaAs photodiodes. At 10 Gbps, the BER is measured at $9.0 \cdot 10^{-10} s^{-1}$.

TABLE I

CORRESPONDENCE BETWEEN PATH STATES AND BB84 STATES.

ϕ	Path State	Defined Pol. State	Defined Bit State
0	$\frac{\|t\rangle + \|b\rangle}{\sqrt{2}}$	$\|\leftrightarrow\rangle$	$\|0_+\rangle$
π	$\frac{\|t\rangle - \|b\rangle}{\sqrt{2}}$	$\|\updownarrow\rangle$	$\|1_+\rangle$
$\pi/2$	$\frac{\|t\rangle + i\|b\rangle}{\sqrt{2}}$	$\|\nearrow\rangle$	$\|0_\times\rangle$
$3\pi/2$	$\frac{\|t\rangle - i\|b\rangle}{\sqrt{2}}$	$\|\nwarrow\rangle$	$\|1_\times\rangle$

C. Single Photon Generation

The technologies mentioned above all use SPDC in order to inject single photons into their photonic device. This method leads to significant losses in performance due to mechanisms such as coupling loss. In order to overcome this, much focus has gone into integrated sources, which removes the need to couple light into their photonic circuit. One common method for the generation of single photons is through spontaneous four-wave mixing (SFWM). SFWM can be realized through the mixing of two or three wavelengths to produce one or two new wavelengths. This process requires the energy to be conserved and is extremely phase sensitive. Therefore, PICs, which are phase-stable, are a good candidate to realize this process. Although it is possible to produce single photons through SFWM, efficiencies are diminished from spectral purity caused from background noise of surrounding components.

In order to overcome the weaknesses of SFWM, an improved design has been adopted by researchers - micro-ring resonators (MRRs) with SFWM [13]. By utilizing MRRs, single-photon generation with high spectral purity and without any filters is possible. This results in higher efficiencies compared to the conventional SFWMs method. Furthermore, by implementing MRRs and SFWMs synergistically, noise can be minimized through a weak optical pump. With only one additional component in the PIC design, the single photon source (SPS) can be simplified and enhanced for scalable applications.

One example of using a MMR with SFWM device is demonstrated by Llewellyn *et al.* [13]. Here, they design and experimentally test a four-photon, four-qubit MRR with SFWM-based single photon generator. By utilizing four identical MRRs within their design, they are able to generate pure and indistinguishable photons with high efficiency while minimizing the background noise from the surrounding components within the circuit. While background noise is minimized by the MRRs, the photons are indistinguishable due to interference created by the Mach Zehnder interferometers (MZIs) within the circuit [13]. In the transmitter circuit, two pairs of non-degenerate photons are generated in the array of MRR SPSs. The four photons are demultiplexed by asymmetric MZIs and routed via waveguide crossings. Utilizing thermal-optic phase shifters on the MZIs allows for the projective measurements of the multi-qubit states. In the receiver circuit, the polarization-encoded qubits are converted to path encoding and then measured by an external avalanche photodetector.

The group experimentally demonstrated signal and idler photons at 1539.758 nm and 1559.015 nm, indicating an ability to achieve single photon generation in the region where silicon has the lowest attenuation. SFWM gain was also measured and background noise was found to be suppressed due to the advantage of having MRRs. Spectral indistinguishability, another parameter of interest, was measured and determined to have a visibility of $90.99 \pm 3.91\%$. Lastly, quantum interference between pairwise MMRs was found to

be excellent with an average of 87.3 $\pm$ 1.9% with multi-pair correction. These results provide a usable and simple design that demonstrates how silicon photonics can be used and scaled for quantum information applications.

D. Single Photon Detection

Many tasks in quantum communications are dependent on single-photon qubits. Due to the very small energies ($\sim 10^{-19}$ J) involved, single photon detectors (SPDs) must be used. Some popular examples of SPDs include avalanche photodiodes, superconducting nanowire single-photon detectors (SNSPDs), and transition edge sensors [14].

One current issue that researchers are attempting to solve is that SPDs can only achieve high efficiencies as an external stand-alone device. Having an external stand-alone device leads to additional losses such as from fibre coupling and material absorption outside the detector [15]. SNSPDs allow for an integrated SPD which provides a unique advantage compared with external devices, as it prevents additional insertion loss mechanisms. Furthermore, SNSPDs have been found to offer high internal quantum efficiencies and low-timing jitter at liquid helium temperature, whereas current alternatives must operate at even colder temperatures in the millikelvin range. Lastly, most integrated devices are compatible with current CMOS fabrication techniques, allowing for easy scalability.

One example of an integrated single-photon detector is demonstrated by Pernice *et al.* [15]. Here, they fabricated and demonstrated a highly efficient and repeatable integrated SPD device at telecom wavelengths. Single photons are first generated externally and coupled into the device, then split at a 50/50 splitter. One path leads to the SNSPD and the other path leads to a control port for baselining, as shown in Figure 3. Remaining light that was not collected by the detector is collected at the residual light port. From their results, they were able to obtain a on-chip single-photon detection efficiency of 91%, dark count rate of 5886 Hz, and a timing jitter of 18 ps. This device presented not only high detection efficiency, but also extremely fast timing jitter, which represents the time it takes for a photon to be absorbed by the detector and converted into electrical signal. Although the dark count rate was found to be high, the researchers noted that the detection rate was within the MHz range, and that dark counts within the kHz range had negligible affect on the detection efficiency. SNSPD designs are constantly being improved, such as the addition of low-loss delay lines to create photon buffering, resulting in increased quantum efficiencies and speed. However, one crucial limitation still remains for the SPD field, which requires extremely low temperature operations to detect single-photons.

IV. Conclusion

While there is still room for improvement in device power and efficiency, silicon photonics provides a platform for tremendously powerful and compact quantum computation devices. As the field continues to evolve, it is likely that devices capable of manipulating a greater number of qubits will emerge. As such devices pose a threat to modern communication security, it is essential to develop quantum-secure alternatives to contemporary quantum-susceptible protocols.

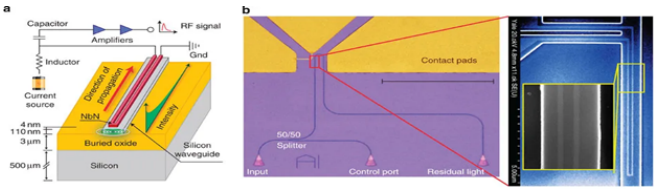

Fig. 3. **a**, SNSPD structure. **b**, Optical micrograph of integrated circuit.

Fortunately, silicon photonics also provides a platform for compact and scalable secure communications techologies. Heterogeneous bonding of active laser materials onto silicon PICs can enable fully integrated QKD transmitters. In addition, the integration of single photon generators and detectors necessary for more advanced tasks in quantum information science can accelerate research and commercialization in the field. These integrated devices will be able to leverage the existing manufacturing processes to achieve the widespread adoption of quantum-secure communications protocols.

References

[1] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Comm. ACM*, 1978.

[2] P. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM J. Sci. Statist. Comput. 26*, vol. 1484, 1994.

[3] D. Coppersmith, "Modifications to the number field sieve," *Journal of Cryptology*, vol. 6, pp. 169–180, 1993.

[4] Y. Takahash and N. Kunihiro, "A quantum circuit for shor's factoring algorithm using 2n + 2 qubits," *Quantum Information and Computation*, vol. 6, no. 2, pp. 184–192, 2006.

[5] F. Arute, K. Arya, R. Babbush *et al.*, "Quantum supremacy using a programmable superconducting processor," *Nature*, vol. 574, p. 505–510, Oct 2019.

[6] B. P. Lanyon, T. J. Weinhold, N. K. Langford, M. Barbieri, D. F. V. James, A. Gilchrist, and A. G. White, "Experimental demonstration of a compiled version of shor's algorithm with quantum entanglement," *Phys. Rev. Lett.*, vol. 99, no. 25, p. 250505, Dec 2007.

[7] A. Polit, J. Matthews, and J. O'Brien, "Shor's quantum factoring algorithm on a photonic chip," *Science*, vol. 325, no. 5945, 2009.

[8] A. Politi, J. C. F. Matthews, and J. L. O'Brien, "Shor's quantum factoring algorithm on a photonic chip," *Science*, vol. 325, no. 1221, p. 250505, Dec 2009.

[9] C. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Proc. IEEE Int. Conf. Computers, Systems and Signal Processing*, pp. 175–179, 1984.

[10] P. Shor and J. Preskill. (2000, May) Simple proof of security of the bb84 quantum key distribution protocol. [Online]. Available: arXiv:quant-ph/0003004

[11] D. Bunandar, A. Lentine, C. Lee *et al.*, "Metropolitan quantum key distribution with silicon photonics," *Phy. Rev. X*, vol. 8, no. 021009, April 2018.

[12] D. Taillaert, H. Chong, P. I. Borel, L. H. Frandsen, R. M. DeLaRue, and R. Baets, "A compact two-dimensional grating coupler used as a polarization splitter," *IEEE Photonics Technology Letters*, vol. 15, no. 9, pp. 1249–1251, 2003.

[13] D. Llewellyn, Y. Ding, I. Faruque *et al.*, "Chip-to-chip quantum teleportation and multi-photon entanglement in silicon," *Nat. Phys.*, vol. 16, p. 148–153, Dec 2020.

[14] R. H. Hadfield, "Single-photon detectors for optical quantum information applications," *Nature Photonics*, vol. 3, pp. 696–705, Dec 2009.

[15] W. Pernice, O. M. C. Schuck *et al.*, "High-speed and high-efficiency travelling wave single-photon detectors embedded in nanophotonic circuits," *Nat. Commun.*, vol. 3, p. 1325, Dec 2012.