Title	Chip-based quantum key distribution
Author(s)	Leong-Chuan Kwek, Lin Cao, Wei Luo, Yunxiang Wang, Shihai Sun, Xiangbin Wang and Ai Qun Liu

Chip-based Quantum Key Distribution

Leong-Chuan Kwek,[1,2,3] Lin Cao,[4,5] Wei Luo,[5,6] Yunxiang Wang,[7] Shihai Sun,[8] Xiangbin Wang,[9,10,11] and Ai Qun Liu*[5,6]

[1] *Centre for Quantum Technologies, National University of Singapore*
[2] *MajuLab, CNRS-UNS-NUS-NTU International Joint Research Unit, Singapore UMI 3654, Singapore*
[3] *National Institute of Education, Nanyang Technological University, Singapore 637616, Singapore*
[4] *Institute of Microelectronics, Peking University, Beijing, China*
[5] *Quantum Science and Engineering Centre (QSec), Nanyang Technological University, Singapore*
[6] *School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore*
[7] *School of Optoelectronic Science and Engineering, University of Electronic Science and Technology of China, Chengdu 610054, China*
[8] *School of Physics and Astronomy, Sun Yat-Sen University, Zhuhai 519082, China*
[9] *State Key Laboratory of Low Dimensional Quantum Physics, Department of Physics, Tsinghua University, Beijing 100084, Peoples Republic of China*
[10] *Synergetic Innovation Center of Quantum Information and Quantum Physics, University of Science and Technology of China Hefei, Anhui 230026, China*
[11] *Jinan Institute of Quantum technology, SAICT, Jinan 250101, Peoples Republic of China*

Quantum key distribution is a matured quantum science and technology. Over the last twenty years, there has been substantial research and development in this area. Recently, silicon technology has offered tremendous promise in the field for improved miniaturization of quantum key distribution through integrated photonic chips. We expect further progress in this area both in terms of protocols, photon sources and photon detectors. This review captures some of the recent advances in this area.

I. INTRODUCTION

The need for secure transmission of information depends crucially on the level of paranoia in an organization. Thus, there has been a need to maintain secure transmission of information within government organizations, especially in defense, or large corporations, especially with regards to trade secrets. Yet, how do we transmit messages securely?

Cryptography, the ancient art of secret writing, has always been a combination of scrambling and confusion. A good scrambling of the plaintexts (messages) is the basis of many symmetric-key encryption schemes, like the Advanced Encryption Standard (AES). There is also asymmetric-key encryption algorithms or public key distribution systems that use a pair of keys, a public key associated with the creator or sender for encrypting messages and a private key that only the receiver (often the originator) knows for decrypting that information. One such public key scheme is the Rivest-Shamir-Adleman (RSA) protocol which relies essentially on the difficulty of factoring two large prime numbers.

Conceived much earlier (at least ten years earlier), but finally published in 1983, Wiesner outlines a protocol for storing quantum money in two conjugate bases:the first one in vertical and horizontal polarization and the second one in right and left circular polarization [1]. Wiesner communicated this idea to Charles Bennett who subsequently proposed a quantum key distribution with Gille Brassard based on the idea of "conjugate" bases [2, 3]. In an independent research, Artur Ekert proposed a different approach to establish a secret key between two parties based on the correlations of two entangled particles[4].

II. QUANTUM KEY DISTRIBUTION

A cryptographic channel comprises of two distant parties that share a communication channel so that they can communicate securely and privately despite the presence of an eavesdropper. The two parties are typically labelled Alice and Bob, two fictitious characters first popularized by the same Rivest, Shamir and Adleman [5] who propounds the RSA scheme. The search for an unbreakable cipher remained the "Holy Grail" of cryptography until 1949 when it was shown that one could achieve secure communication theoretically via the one-time-pad (OTP) method (Vernam, 1926) as long as the two users, Alice and Bob, share a sufficiently long random string that is kept secret from Eve. Note that for the OTP scheme to be theoretically secured, it is important that the random string used as the one-time pad is as long as the message itself, and that it is used once and never reused [6].

The protocol of distributing such a long key in a one-time pad in the presence of an eavesdropper, typically called Eve, is known as the key distribution problem. Traditionally, such one-time pad are carefully duplicated and distributed to two distant parties through various means, like through a courier, for instance. However, this distribution method suffers from various espionage tactics and it is never very secure. Moreover, once an eavesdropper has access to the one-time pad, he or she can easily copy the contents without either Alice or Bob knowing.

In this review, we survey the landscape for chip-based quantum key distribution. We focus primarily on our two recent work in the area: one on continuous variable QKD and another on measurement device independent (MDI)-QKD.

III. CHIP-BASED TECHNOLOGIES

The spectacular success of microelectronics has shown that there is an enormous potential for turning basic physics into applications through miniaturization. Silicon photonic technology offers many unparalleled benefits including small size, low cost, low power consumption, and well-established batch fabrication techniques[7]. Indium phosphide (InP)[8], lithium niobate ($LiNbO_3$)[9] and potassium titanyl phosphate (KTP)[10] have been used to fabricate on-chip lasers and fast modulators. Silica offers low-loss delay lines and fibre-chip couplers, but lacks rapid modulation [11, 12]. Silicon relies on well-established microfabrication techniques and is ideally suited for both on-chip photonic components [13–15].

IV. BB84

The theory behind BB84 is well documented [16–20]. Alice randomly transmit random bits based on one of the two bases: $\{|H\rangle, |V\rangle\}$ or $\{|+\rangle, |-\rangle\}$ corresponding to bits $\{|0\rangle, |1\rangle\}$ respectively. When Bob receives the photon, he randomly selects one of the two bases to measure. Naturally, if he selects the correct basis, he gets the correct transmitted bit. However, if he does not selects the correct basis, he incurs an error. Alice and Bob then reveal their bases but not their transmitted bits and discard all bits in which Alice and Bob uses different bases. On average, half of the bits transmitted are lost. To ensure further safety in the transmission, they then chooses to verify their bits (by revealing their bit publicly) and immediately discard those bits. This is the process of reconciliation. If there is no eavesdropper, they should always agree on these bits. Any deviation from perfect fit then gives them an idea on the amount of eavesdropping.

The BB84 protocol has been demonstrated experimentally with linear optics over long distances through optical fibers and free space. The first experiment is done with Alice controlling two pockel cells so that she is able to transmit the four polarization states [17]. Since then, there have been many experimental confirmation of QKD over longer and longer distances through fibers [21, 22], free space [23, 24], and satellites [25–27].

In Ref. [8], the BB84 QKD protocol is implemented with time-bin encoding on a chip. In this scheme, the state $|0\rangle$ is encoded by a photon in the first time-bin and the state $|1\rangle$ is encoded by a photon in the second time-bin. The state $|+\rangle$ is encoded as a superposition of the first and second time-bin photon with zero relative phase. The state $|-\rangle$ is encoded as superposition of being in the first and second time-bin with a relative phase of π. The BB84 protocol transmits one of two orthogonal states chosen at random, encoded in one of two randomly chosen non-orthogonal bases: the Z-basis $\{|0\rangle, |1\rangle\}$ and the X-basis $\{|+\rangle, |-\rangle\}$.

In Ref. [8], the BB84 QKD protocol is implemented with time-bin encoding on a chip. In this scheme, the state $|0\rangle$ is encoded by a photon in the first time-bin and the state $|1\rangle$ is encoded by a photon in the second time-bin. The state $|+\rangle$ is encoded as a superposition of the first and second time-bin photon with zero relative phase. The state $|-\rangle$ is encoded as superposition of being in the first and second time-bin with a relative phase of π. The BB84 protocol transmits one of two orthogonal states chosen at random, encoded in one of two randomly chosen non-orthogonal bases: the Z-basis $\{|0\rangle, |1\rangle\}$ and the X-basis $\{|+\rangle, |-\rangle\}$.

In the experiment, the InP-based transmitter chip comprises an on-chip tunable laser, formed from two distributed Bragg reflectors (DBR) and a semiconductor optical amplifier (SOA). The continuous wave singel mode laser source has a coherence time > 1.5 ns, a side-mode suppression ratio of > 50 dB and an operating wavelength of 1,550 nm with B10 nm tuning range. Short electrical pulses applied to the reverse biased EOPM in the first Mach–Zehnder interferometer (MZI) enabled optical pulse generation with < 150 ps duration and B30 dB extinction ratio.

The receiver chip comprises alternating layers of Si_3N_4 and SiO_2 and etched to create a waveguide structure to guide light with a high index-contrast but low loss (B0.5 dB/cm), and a low coupling loss between chip and fibre (B2 dB), yielding a total loss B9 dB for BB84 configuration.

In Ref. [8], they actually implemented three different protocols: BB84, coherent one-way (COW) [28] and differential phase shift (DPS) [29]. In all cases, performances comparable to the state-of-the-art current fibre and bulk optical systems have been achieved with a key rates of 345 kbps (BB84), 311 kbps (COW) [8] and 565 kbps (DPS). Similar experiments have been demonstrated elsewhere [30–33].

V. MDI-QKD

A. Theory

Measurement-device-independent quantum key distribution (MDI-QKD) employs an untrusted relay to prevent the communication channel from side-channel attacks commonly encountered in earlier QKD protocols.

To understand MDI-QKD, we follow the nice description in Ref. [34]. To do this, we first introduce an Einstein-Podolsky-Rosen (EPR) based QKD protocol. Alice and Bob first prepares an EPR pair and sends half of it to an untrusted third party, Charles. Charles then performs an entanglement swapping operation [35, 36] on the incoming signals via a Bell state measurement (BSM), and then broadcast his measurement results. On completion of the measurement, Alice and Bob measure their halves of the EPR pairs with two conjugate bases (the rectilinear basis Z, or the diagonal basis X) that they select at random. By doing so they can determine

whether or not Charles is honest. For this, they can compare a randomly chosen subset of their data to test if it satisfies the expected correlations associated with the Bell state declared by Charles.

As shown in the excellent review, Ref. [37], this protocol can also be implemented in a "time-reversal" fashion. This is so because Charles' operations commute with those of Alice and Bob. Therefore, one can reverse the order of the measurements. That is, it is not necessary that Alice and Bob wait for Charles's results in order to measure their halves of the EPR pairs, but they can measure them beforehand. Note that Charles' BSM is only used to check the parity of Alice's and Bob's bits and, therefore, it does not reveal any information about the individual bit values. This rephrases the original EPR based QKD protocol into an equivalent prepare-and-measure scheme where Alice and Bob directly send Charles BB84 states and Charles performs the measurements. Most importantly, like in the original EPR based QKD protocol, Alice and Bob can test the honesty of Charles by just comparing a random portion of their signals.

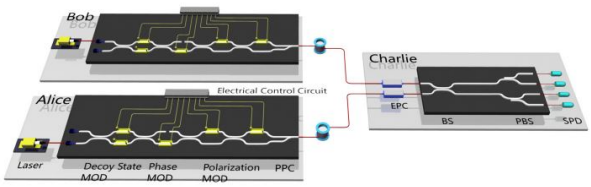

FIG. 1. Schematic diagram of the silicon photonic chip-based MDI QKD system. The system comprises three silicon photonic chips (Alice, Bob, and Charlie) among which Alice and Bob chips are the transmitters and Charlie chip is the server. Alice and Bob chips consist of intensity modulators, phase modulators, and polarization modulators, which are capable of generating phase-randomized signal and decoy-state weak coherent pulses in BB84 polarization states. Charlie's chip is made up of a polarization-independent beam splitter and two polarizing beam splitters and it is capable of performing Bell state measurement of the incoming states with off-chip single-photon detectors (SPDs). MOD, modulator; PPC, path-to-polarization converter; EPC, electrically driven polarization controller.

B. Experiment

Experimental demonstration of MDI-QKD has been performed in Refs. [38, 39] with bulk optics over long distances. The set-ups are ideal for a quantum network. In Ref. [38], a time-bin phase-encoding MDI-QKD scheme is realized whereas in Ref. [39], the researchers assess the feasibility of MDI-QKD using the decoy-state protocol proposed by Wang [40].

Recently we have realized a fully chip-based MDI-QKD system (see Fig. 1). We were not the only group to do it on photonic chip. There are also two other excellent pieces of work: the first in China led by Feihu Xu and Jianwei Pan [41] and the second in Bristol led by Mark Thompson, John Rarity and Chris Erven[42]. Here, we describe our system. Our system comprises two transmitter chips (Alice and Bob) and one receiver chip (Charlie). The key components of the transmitter chip are the intensity modulators for the decoy states, phase modulators and polarization modulators. These devices are fully integrated into a single chip. The receiver chip integrates polarization-independent beam splitters (BS) and polarizing beam splitters (PBS). In our experiment, we demonstrate a key rate per pulse of 2.923×10^{-6} which is sufficient for low-error quantum communications.

For the transmitter chip, a pulse-modulated 1542.3815-nm frequency-locked laser is coupled into the silicon waveguide through a grating coupler. The first Mach-Zehnder interferometer (MZI) modulator modifies the laser intensity to create signal and decoy states, and another phase modulator implements random phase modulations of the input pulses. Polarization states $|H\rangle, |V\rangle, |+\rangle$ and $|-\rangle$ are encoded by a polarization modulator consisting of an MZI modulator, a path-to-polarization convertor (PPC), and phase shifters at the PPC input arms. Light is coupled out of the chip through an adiabatic tapered waveguide coupler and a lensed fibre with a $3-\mu$m spot diameter. The edge coupler is designed with a cross-section of 200nm $\times$ 220nm to minimize the polarization-dependent loss (PDL). After attenuation, the weak coherent pulses from the two transmitter chips reach the receiver chip (Charlie) via optical fiber spools. The receiver chip consists of a polarization-independent BS and two PBS. Before entering the receiver chip, the pulses are compensated for polarization drift by polarization controllers in order to maximize the Hong-Ou-Mandel (HOM) interference between the transmitted photons from Alice and Bob chips. Finally, Bell states are measured with single-photon detectors, and all coincidence events for secure key generation are publicly announced. The security of MDI-QKD is guaranteed because the measured outcomes do not contain any information on the secret key encoding.

Both the MDI-QKD transmitter and receiver chips were designed and fabricated by using advanced silicon photonic fabrication techniques, which utilized silicon-on-insulator (SOI) wafer with a top silicon layer of 220 nm and a buried oxide layer (BOX) of 3 μm. The top silicon was etched to form grating coupler. Slab layer of ridge waveguide in PPC and other components were fabricated using inductively coupled plasma-reactive ion etching (ICP-RIE). Subsequently, strip waveguide was formed by etching through the remaining silicon. On completion of the waveguide etching, silicon oxide was deposited on the silicon chip. Titanium nitride (TiN) is then added to form the waveguide heaters. Aluminum (Al) was then deposited to provide the necessary electrical connection between external power source and waveguide heaters. Finally, we etch isolation trenches in order to prevent thermal crosstalk between adjacent heaters.

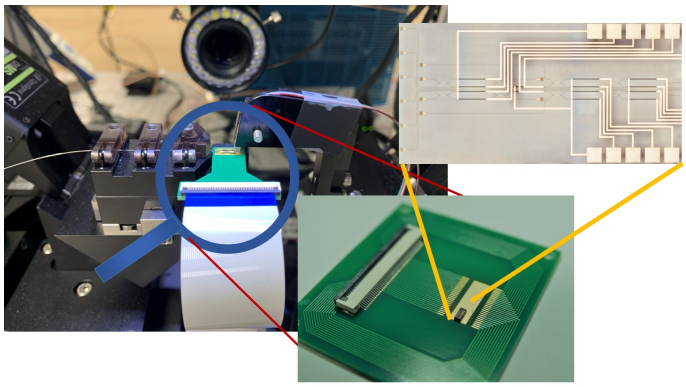

FIG. 2. Picture showing the size of the MDI-QKD chip with integrated photonic circuits together with the peripheral set up. Insets shows the zoom-in version of the tiny chip.

The intensity modulators, phase modulators and polarization modulators were integrated onto a single transmitter chip. Figures 2a and 2b illustrate the optical micrographs of the transmitter and receiver chip, respectively. Figure 2c shows the transmitter chip packaged on a printed circuit board (PCB).

The MDI-QKD architecture is naturally suited for multi-user QKD networks [43], since the most expensive and intricate component - the measurement device - can be placed in an untrusted relay and shared among many QKD users. Therefore, MDI-QKD has been widely recognized as a promising quantum communication technology for star-type secured networks[34, 44].

VI. CV-QKD

Continuous variable QKD or CV QKD refers to quantum communication with weak coherent pulses and homodyne detections. Compared with discrete variable QKD, continuous variable QKD appears to be more suitable for photonic chip integration due to its compatibility with existing telecom technologies. The advantages and disadvantages of Discrete QKD and CV QKD is well-documented [45, 46]. Yet, the security analysis of this technique is a lot more complicating compared to discrete-variable QKD despite the simplicity in the actual protocol.

There are two prepare-and-measure continuous variable QKD or Gaussian QKD: (i) an entanglement based scheme using two-mode squeezed states and (ii) a scheme based on coherent states and heterodyne detections.

In the entanglement-based scheme, Alice prepares a two-mode squeezed vacuum state. Alice prepares a coherent state, whose displacement vector is Gaussian distributed in x and p, by applying a heterodyne measurement at her share of the two-mode squeezed state. Bob then applies a homodyne measurement on mode B, measuring quadrature x or p.

Experimental CV QKD has already been performed over long distances of 80 to 100 km [47, 48].

In Ref. [9], we provided a proof-of-principle chip-based CV-QKD system that is capable of producing a secret key rate of 0.14 kbps (under collective attack) over a simulated distance of 100 km in fibre, offering new possibilities for low-cost, scalable and portable quantum networks.

Figure 3 shows a schematic of the silicon photonic CV-QKD chip. The transmitter chip (Alice) comprises of a 1,550-nm continuous-wave laser coupled into the waveguide with a grating coupler. The first modulator serves as an attenuator to control the input laser intensity. We split the input laser into two paths, with the weaker one as signal and the stronger one as the local oscillator (LO) using a 1:99 directional coupler. The signal path is then modulated with an amplitude modulator (AM) and a phase modulator (PM) to generate a series of coherent state $|x_A + ip_A\rangle$, where x_A and p_A are Gaussian ditributed random numbers. A digital filter and demodulator extract the information from one of the sideband frequencies. To keep the relative phase between the signal path and the local oscillator (LO) path after transmission, the modulated signal and LO are multiplexed into two orthogonal polarization states with a two-dimensional grating coupler. Information encoding is one through a modulation of the continuous light signal on the sideband ranging from 1–10 MHz as in Ref. [49, 50]. After the signal is transmitted over a line with a transmittance T, the receiver (Bob) first compensates the polarization drift with a polarization controller followed by demultiplexing of the signal and the LO with another two-dimensional grating coupler. Finally, Bob arbitrarily measures x or p quadrature with the homodyne detector and also filters out the required frequency. The security of CV-QKD is guaranteed by the Heisenberg uncertainty principle between the x and p quadratures. Because the two quadratures do not commute, any attempt by the eavesdropper's (Eve) to measure one quadrature would result in noise in the other, which implies that the amount of information of the key leaked to Eve is bound by the noise level detected by Alice and Bob if Eve do not wish to be detected.

In our experiment, the homodyne detection efficiency is $\eta = 0.498$. There is also 5-dB loss of Bob's chip due to an additional 68.3% drop in efficiency. The total excess noise is $\epsilon = 0.0934$ shot-noise units (SNU) at a modulation variance of $V_{mod} = 7.07$ SNU and $T = 1$. Detector electrical noise is $\nu_{el} = 0.0691$ SNU. Symbol rate is $SR = 0.8$ Mbps. With these data, the secure key rate of the current CV-QKD system can be estimated. At 90 km, the Shannon raw key rate and Holevo raw key rate are both roughly 10^3. Fig. 4 shows the reconciliation efficiency and signal to noise ratio (SNR) values. The secure fraction and the calculated SNR is plotted as a function of transmission distance. These values are comparable to existing benchmarks.

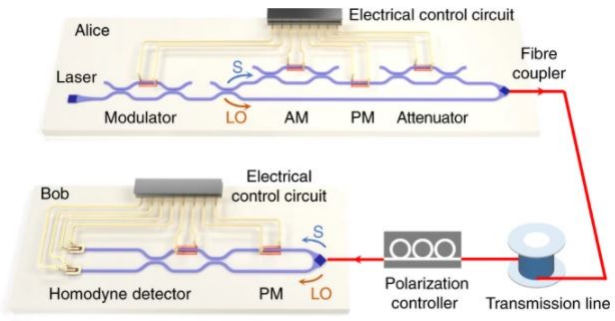

FIG. 3. The silicon photonic chips comprises of two parts, Alice and Bob, which are used as the transmitter and receiver. Alice's side consists of several AMs, PMs, attenuators and grating couplers, which can modulate the signal (S) and multiplex the signal with the LO in two orthogonal polarization states. Bob demultiplexes and detects the signal with the receiver chip.

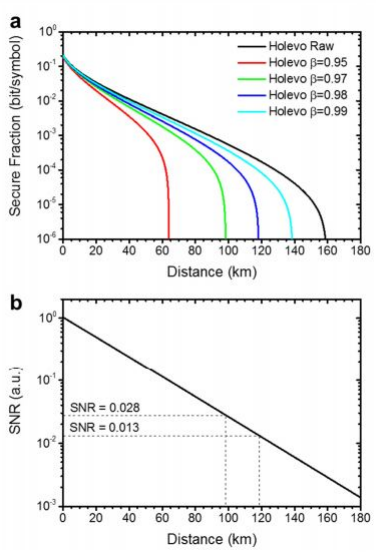

FIG. 4. Reconciliation efficiency and SNR considerations. a The secure fraction as a function of transmission distance. b The calculated SNR at different simulated fibre transmission distance.

VII. OVERALL PROSPECT AND CONCLUSION

Integrated photonics continue to offer one of the most stable, compact and robust platforms to miniaturize massive photonic circuits [51]. The mature fabrication processes of silicon chips and its full compatibility with electronic circuits are also advantages for a compact device. This compactness and compatibility with classical devices would also allow QKD devices to be embedded into classical devices without easy detection. Overall, chip based technologies offer advantages in size compactness, low energy consumption, and a potential for low cost [7, 45].

With no electro-optical nonlinearity, many silicon photonic chips currently utilize slow thermo-optical phase modulators for high fidelity state preparation [52]. Yet, high-speed modulation of quantum states in standard silicon photonics appears possible in the near future with carrier- injection and carrier-depletion modulators even though the latter currently does not quite work well in quantum applications. These limitations can however be overcome [52].

Finally, the compatibility of integrated photonic chips with current integrated photonic telecommunication hardware may allow for seamless operation alongside classical communications transceivers, enabling hybrid classical and quantum communications devices [52].

VIII. ACKNOWLEDGMENT

This work was supported by the Singapore Ministry of Education (MOE) Tier 3 grant (MOE2017-T3-1-001), the Singapore National Research Foundation (NRF) National Natural Science Foundation of China (NSFC) joint grant (NRF2017NRF-NSFC002-014) and the Singapore National Research Foundation under the Competitive Research Program (NRF-CRP13-2014-01).

IX. AUTHOR CONTRIBUTIONS

All authors contributed equally to the review.

[1] Stephen Wiesner. Conjugate coding. *ACM Sigact News*, 15(1):78–88, 1983.
[2] Charles H Bennett and Gilles Brassard. Proceedings of the ieee international conference on computers, systems and signal processing, 1984.
[3] Gilles Brassard. Brief history of quantum cryptography: A personal perspective. In *IEEE Information Theory Workshop on Theory and Practice in Information-Theoretic Security, 2005.*, pages 19–23. IEEE, 2005.
[4] Artur K Ekert. Quantum cryptography based on bell's theorem. *Physical Review Letters*, 67(6):661, 1991.
[5] Ronald L. Rivest, Adi Shamir, and Leonard Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 26(1):96–99, 1983.
[6] Claude E Shannon. Communication theory of secrecy systems. *The Bell system technical journal*, 28(4):656–715, 1949.

[7] Adeline Orieux and Eleni Diamanti. Recent advances on integrated quantum communications. *Journal of Optics*, 18(8):083002, 2016.

[8] Philip Sibson, Chris Erven, Mark Godfrey, Shigehito Miki, Taro Yamashita, Mikio Fujiwara, Masahide Sasaki, Hirotaka Terai, Michael G Tanner, Chandra M Natarajan, et al. Chip-based quantum key distribution. *Nature communications*, 8(1):1–6, 2017.

[9] Gong Zhang, Jing Yan Haw, Hong Cai, Feng Xu, SM Assad, Joseph F Fitzsimons, Xianzhong Zhou, Y Zhang, S Yu, J Wu, et al. An integrated silicon photonic chip platform for continuous-variable quantum key distribution. *Nature Photonics*, 13(12):839–842, 2019.

[10] Sébastien Tanzilli, Anthony Martin, Florian Kaiser, Marc P De Micheli, Olivier Alibart, and Daniel B Ostrowsky. On the genesis and evolution of integrated quantum optics. *Laser & Photonics Reviews*, 6(1):115–143, 2012.

[11] Alberto Politi, Martin J Cryan, John G Rarity, Siyuan Yu, and Jeremy L O'brien. Silica-on-silicon waveguide quantum circuits. *Science*, 320(5876):646–649, 2008.

[12] K Miura Davis, Kiyotaka Miura, Naoki Sugimoto, and Kazuyuki Hirao. Writing waveguides in glass with a femtosecond laser. *Optics letters*, 21(21):1729–1731, 1996.

[13] Jian Guo Huang, Hong Cai, YD Gu, Lip Ket Chin, Jiu Hui Wu, Tian Ning Chen, Zheng Chuan Yang, Yi Long Hao, and Ai Qun Liu. Torsional frequency mixing and sensing in optomechanical resonators. *Applied Physics Letters*, 111(11):111102, 2017.

[14] Yu Zhi Shi, Sha Xiong, Yi Zhang, Lip Ket Chin, Y-Y Chen, Jing Bo Zhang, TH Zhang, Wee Ser, A Larrson, SH Lim, et al. Sculpting nanoparticle dynamics for single-bacteria-level screening and direct binding-efficiency measurement. *Nature communications*, 9(1):1–11, 2018.

[15] Yuzhi Shi, Sha Xiong, Lip Ket Chin, Jingbo Zhang, Wee Ser, Jiuhui Wu, Tianning Chen, Zhenchuan Yang, Yilong Hao, Bo Liedberg, et al. Nanometer-precision linear sorting with synchronized optofluidic dual barriers. *Science advances*, 4(1):eaao0773, 2018.

[16] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden. Quantum cryptography. *Reviews of Modern Physics*, 74(1):145, 2002.

[17] Charles H Bennett, François Bessette, Gilles Brassard, Louis Salvail, and John Smolin. Experimental quantum cryptography. *Journal of cryptology*, 5(1):3–28, 1992.

[18] Richard J Hughes, Douglas M Alde, P Dyer, Gabriel G Luther, George L Morgan, and M Schauer. Quantum cryptography. *Contemporary Physics*, 36(3):149–163, 1995.

[19] Charles H Bennett, Gilles Brassard, and Artur K Ekert. Quantum cryptography. *Scientific American*, 267(4):50–57, 1992.

[20] Peter W Shor and John Preskill. Simple proof of security of the bb84 quantum key distribution protocol. *Physical Review Letters*, 85(2):441, 2000.

[21] Danna Rosenberg, Jim W Harrington, Patrick R Rice, Philip A Hiskett, Charles G Peterson, Richard J Hughes, Adriana E Lita, Sae Woo Nam, and Jane E Nordholt. Long-distance decoy-state quantum key distribution in optical fiber. *Physical review letters*, 98(1):010503, 2007.

[22] Cheng-Zhi Peng, Jun Zhang, Dong Yang, Wei-Bo Gao, Huai-Xin Ma, Hao Yin, He-Ping Zeng, Tao Yang, Xiang-Bin Wang, and Jian-Wei Pan. Experimental long-distance decoy-state quantum key distribution based on polarization encoding. *Physical review letters*, 98(1):010505, 2007.

[23] J Wabnig, D Bitauld, HW Li, A Laing, JL O'brien, and AO Niskanen. Demonstration of free-space reference frame independent quantum key distribution. *New Journal of Physics*, 15(7):073001, 2013.

[24] Tobias Schmitt-Manderbach, Henning Weier, Martin Fürst, Rupert Ursin, Felix Tiefenbacher, Thomas Scheidl, Josep Perdigues, Zoran Sodnik, Christian Kurtsiefer, John G Rarity, et al. Experimental demonstration of free-space decoy-state quantum key distribution over 144 km. *Physical Review Letters*, 98(1):010504, 2007.

[25] Sheng-Kai Liao, Wen-Qi Cai, Wei-Yue Liu, Liang Zhang, Yang Li, Ji-Gang Ren, Juan Yin, Qi Shen, Yuan Cao, Zheng-Ping Li, et al. Satellite-to-ground quantum key distribution. *Nature*, 549(7670):43–47, 2017.

[26] Giuseppe Vallone, Davide Bacco, Daniele Dequal, Simone Gaiarin, Vincenza Luceri, Giuseppe Bianco, and Paolo Villoresi. Experimental satellite quantum communications. *Physical Review Letters*, 115(4):040502, 2015.

[27] Robert Bedington, Juan Miguel Arrazola, and Alexander Ling. Progress in satellite quantum key distribution. *npj Quantum Information*, 3(1):1–13, 2017.

[28] Damien Stucki, Nicolas Brunner, Nicolas Gisin, Valerio Scarani, and Hugo Zbinden. Fast and simple one-way quantum key distribution. *Applied Physics Letters*, 87(19):194108, 2005.

[29] Toshimori Honjo, Hiroki Takesue, and Kyo Inoue. Differential-phase quantum key distribution experiment using a series of quantum entangled photon pairs. *Optics letters*, 32(9):1165–1167, 2007.

[30] Darius Bunandar, Anthony Lentine, Catherine Lee, Hong Cai, Christopher M Long, Nicholas Boynton, Nicholas Martinez, Christopher DeRose, Changchen Chen, Matthew Grein, et al. Metropolitan quantum key distribution with silicon photonics. *Physical Review X*, 8(2):021009, 2018.

[31] Chaoxuan Ma, Wesley D Sacher, Zhiyuan Tang, Jared C Mikkelsen, Yisu Yang, Feihu Xu, Torrey Thiessen, Hoi-Kwong Lo, and Joyce KS Poon. Silicon photonic transmitter for polarization-encoded quantum key distribution. *Optica*, 3(11):1274–1278, 2016.

[32] Joshua W Silverstone, J Wang, D Bonneau, P Sibson, R Santagati, C Erven, JL O'Brien, and MG Thompson. Silicon quantum photonics. In *2016 International Conference on Optical MEMS and Nanophotonics (OMN)*, pages 1–2. IEEE, 2016.

[33] Taofiq K Paraïso, Innocenzo De Marco, Thomas Roger, Davide G Marangon, James F Dynes, Marco Lucamarini, Zhiliang Yuan, and Andrew J Shields. A modulator-free quantum key distribution transmitter chip. *NPJ Quantum Information*, 5(1):1–6, 2019.

[34] Feihu Xu, He Xu, and Hoi-Kwong Lo. Protocol choice and parameter optimization in decoy-state measurement-device-independent quantum key distribution. *Physical Review A*, 89(5):052333, 2014.

[35] Jian-Wei Pan, Dik Bouwmeester, Harald Weinfurter, and Anton Zeilinger. Experimental entanglement swapping: entangling photons that never interacted. *Physical Review Letters*, 80(18):3891, 1998.

[36] Marek Zukowski, Anton Zeilinger, Michael A Horne, and Aarthur K Ekert. " event-ready-detectors" bell experiment via entanglement swapping. *Physical Review Let-*

ters, 71(26), 1993.

[37] Feihu Xu, Marcos Curty, Bing Qi, and Hoi-Kwong Lo. Measurement-device-independent quantum cryptography. *IEEE Journal of Selected Topics in Quantum Electronics*, 21(3):148–158, 2014.

[38] Yang Liu, Teng-Yun Chen, Liu-Jun Wang, Hao Liang, Guo-Liang Shentu, Jian Wang, Ke Cui, Hua-Lei Yin, Nai-Le Liu, Li Li, et al. Experimental measurement-device-independent quantum key distribution. *Physical Review Letters*, 111(13):130502, 2013.

[39] Allison Rubenok, Joshua A Slater, Philip Chan, Itzel Lucio-Martinez, and Wolfgang Tittel. Real-world two-photon interference and proof-of-principle quantum key distribution immune to detector attacks. *Physical Review Letters*, 111(13):130501, 2013.

[40] Xiang-Bin Wang. Three-intensity decoy-state method for device-independent quantum key distribution with basis-dependent errors. *Physical Review A*, 87(1):012320, 2013.

[41] Kejin Wei, Wei Li, Hao Tan, Yang Li, Hao Min, Wei-Jun Zhang, Hao Li, Lixing You, Zhen Wang, Xiao Jiang, et al. High-speed measurement-device-independent quantum key distribution with integrated silicon photonics. *Physical Review X*, 10(3):031030, 2020.

[42] Henry Semenenko, Philip Sibson, Andy Hart, Mark G Thompson, John G Rarity, and Chris Erven. Chip-based measurement-device-independent quantum key distribution. *Optica*, 7(3):238–242, 2020.

[43] Lingwen Kong, Zhihao Li, Congxiu Li, Lin Cao, Zeyu Xing, Junqin Cao, Yaxin Wang, Xinlun Cai, and Xiaoqi Zhou. Photonic integrated quantum key distribution receiver for multiple users. *Optics Express*, 28(12):18449–18455, 2020.

[44] Bernd Fröhlich, James F Dynes, Marco Lucamarini, Andrew W Sharpe, Zhiliang Yuan, and Andrew J Shields. A quantum access network. *Nature*, 501(7465):69–72, 2013.

[45] Feihu Xu, Xiongfeng Ma, Qiang Zhang, Hoi-Kwong Lo, and Jian-Wei Pan. Secure quantum key distribution with realistic devices. *Reviews of Modern Physics*, 92(2):025002, 2020.

[46] Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J Cerf, Miloslav Dušek, Norbert Lütkenhaus, and Momtchil Peev. The security of practical quantum key distribution. *Reviews of modern physics*, 81(3):1301, 2009.

[47] Paul Jouguet, Sébastien Kunz-Jacques, and Anthony Leverrier. Long-distance continuous-variable quantum key distribution with a gaussian modulation. *Physical Review A*, 84(6):062317, 2011.

[48] Paul Jouguet, Sébastien Kunz-Jacques, Anthony Leverrier, Philippe Grangier, and Eleni Diamanti. Experimental demonstration of long-distance continuous-variable quantum key distribution. *Nature photonics*, 7(5):378–381, 2013.

[49] Andrew M Lance, Thomas Symul, Vikram Sharma, Christian Weedbrook, Timothy C Ralph, and Ping Koy Lam. No-switching quantum key distribution using broadband modulated coherent light. *Physical review letters*, 95(18):180503, 2005.

[50] Yong Shen, Hongxin Zou, Liang Tian, Pingxing Chen, and Jianmin Yuan. Experimental study on discretely modulated continuous-variable quantum key distribution. *Physical Review A*, 82(2):022317, 2010.

[51] Jianwei Wang, Fabio Sciarrino, Anthony Laing, and Mark G Thompson. Integrated photonic quantum technologies. *Nature Photonics*, 14(5):273–284, 2020.

[52] Philip Sibson, Jake E Kennard, Stasja Stanisic, Chris Erven, Jeremy L O'Brien, and Mark G Thompson. Integrated silicon photonics for high-speed quantum key distribution. *Optica*, 4(2):172–177, 2017.