entropy

MDPI

Review

Advances in Chip-Based Quantum Key Distribution

Qiang Liu [1], Yinming Huang [1], Yongqiang Du [2], Zhengeng Zhao [2], Minming Geng [1], Zhenrong Zhang [1] and Kejin Wei [2,*]

[1] Guangxi Key Laboratory of Multimedia Communications and Network Technology, School of Computer, Electronics and Information, Guangxi University, Nanning 530004, China
[2] Guangxi Key Laboratory for Relativistic Astrophysics, School of Physical Science and Technology, Guangxi University, Nanning 530004, China
* Correspondence: kjwei@gxu.edu.cn

Abstract: Quantum key distribution (QKD), guaranteed by the principles of quantum mechanics, is one of the most promising solutions for the future of secure communication. Integrated quantum photonics provides a stable, compact, and robust platform for the implementation of complex photonic circuits amenable to mass manufacture, and also allows for the generation, detection, and processing of quantum states of light at a growing system's scale, functionality, and complexity. Integrated quantum photonics provides a compelling technology for the integration of QKD systems. In this review, we summarize the advances in integrated QKD systems, including integrated photon sources, detectors, and encoding and decoding components for QKD implements. Complete demonstrations of various QKD schemes based on integrated photonic chips are also discussed.

Keywords: quantum key distribution; integration technologies; chip-based QKD

Citation: Liu, Q.; Huang, Y.; Du, Y.; Zhao, Z.; Geng, M.; Zhang, Z.; Wei, K. Advances in Chip-Based Quantum Key Distribution. *Entropy* **2022**, *24*, 1334. https://doi.org/10.3390/e24101334

Academic Editors: Pierpaolo Boffi and Mario Martinelli

Received: 30 July 2022
Accepted: 15 September 2022
Published: 22 September 2022

1. Introduction

1.1. Secure Communication

With the rapid development of communication technologies and computing science, communication systems and associated information-processing technologies have been widely used in engineering, commerce, and all aspects of human daily life. However, informatization brings not only convenience and efficiency, but also security risks. For instance, Microsoft Exchange Server vulnerabilities have been exploited, and resulted in tens of thousands of enterprises being attacked [1]. Cyberattacks in Iran led to the mass closures of gas stations across the country [2]. The supervisory control and data acquisition system of Florida drinking water-treatment facilities were invaded, and residents' lives were threatened [3]. Cyberwarfare can undermine the security of critical infrastructures and have a significant impact on the global economy and human life. The security of cyberentities is considered as an important national strategic priority.

The confidentiality of information is an extremely important link of network security. The information cryptography used in modern communication systems based on the assumption of the unidirectional properties of some mathematical analyses, such as the decomposition of large numbers or the solution of discrete logarithms. In other words, the forward calculation (encryption process) of these mathematical problems is very simple, whereas the reverse calculation (decryption process) is extremely complex. Hence, the computation of solving eavesdropping-related problems will be far greater than that of solving encryption-related problems. Even if an eavesdropper's computing capacity is much better than that of the encryptor, she cannot complete the decoding within the secrecy period of transmitted messages. However, with the development of computing science, the promotion of computing capability has far exceeded the initial imagination, so the security of current cryptography may no longer be reliable. In particular, quantum computing theoretically smashes the assumption of computational unidirectionality of mathematical

analyses, which is the basic principle of traditional cryptography. Recently, small-scale quantum computers and quantum supremacy have been reported [4–8]. Although the realization of large-scale quantum computers may be decades away, its potential threat to current information security cannot be ignored. Interestingly, before people realized that quantum computers could be used to crack the current cryptographic systems, they had found approaches to deal with this threat.

Broadly speaking, there are three methods to the quantum secure encryption scheme. One method is to continue using the traditional public key cryptography but develop alternative algorithms to resist quantum attacks. This method is named postquantum cryptography (PQC) [9]. Its technological merit is that it can be compatible with existing cryptoinfrastructure, and it has usable high key rates over long distances. One shortcoming of PQC is that the developed algorithms have been proven to be safe only against known quantum attacks. This may result in future security vulnerabilities with potential disaster for information transmitted today.

The second method is quantum secure direct communication (QSDC), which was first proposed by Long and Liu in 2002 [10] based on quantum laws. QSDC allows users to directly transmit private information over secure quantum channels without security key distribution. Due to its relatively simple communication steps, QSDC has drawn great attention and has experienced rapid development [11–14] over the past two decades. However, the achieved key rates of QSDC [15–18] are rather lower than other quantum secure encryption schemes.

Another method is quantum key distribution (QKD) [19]. The unconditional security of QKD has been rigorously proven [20] based on quantum fundamental laws, such as quantum indistinguishability and the no-cloning theorem. Thus, its safety is independent of future improvements in computing capacity and algorithms. QKD combined with PQC is a typical quantum security scheme the safety of which can be theoretically proven at present. This scheme can instantly discover eavesdropping behaviors and events, and realize high-security and high-performance encryption systems.

1.2. Quantum Key Distribution

The QKD is a technique that allows two remote communication terminals to share a common secret key for cryptographic purposes. During the transmission between two parties (usually called Alice and Bob), an eavesdropper (usually called Eve) may eavesdrop on the quantum communication channel that spies on potential secret key bits. Eve unavoidably introduces disturbances to the transmitting quantum messages based on appropriate quantum laws, e.g., the quantum no-cloning theorem or Heisenberg uncertainty principle. Then the eavesdropping will be detected by the communicators and they can abandon such a key simply, then start new QKD process.

The first QKD scheme is named the BB84 protocol, which was originally proposed by Bennett and Brassard in 1979 and published in 1984 in a computer conference proceedings [19]. The well-known B92 protocol [21] is a version of the BB84 protocol revised in a cryptographic manner, and their physical natures are different. Both BB84 and B92 protocols are invented based on the indistinguishability properties of two arbitrary nonorthogonal qubits in a Hilbert space. In this paper, we refer the protocols, which are developed in a two-dimensional Hilbert space, as qubit-based QKD schemes. Other qubit-based QKD schemes include differential phase shift (DPS) [22] and coherent one way (COW) [23].

Although early QKD protocols use unentangled qubits as quantum information carriers, assorted protocols were proposed by using entanglement qubits [24] or qudits [25–31] instead. Qudit-based QKDs are developed in high-dimensional Hilbert spaces, and thus are also referred to as high-dimensional (HD) QKDs.

Generally, QKDs can be divided into two categories—discrete variable (DV) QKDs and continuous variable (CV) QKDs. We consider qubit-based and qudit-based QKDs as DV-QKDs. Unlike DV-QKD, the Hilbert space of the quantum state used for encryption in CV-QKD is infinite-dimensional and continuous.

Although QKD schemes own unconditional security in theory, there are still some security vulnerabilities in the practical QKD systems due to device imperfections. This issue was theoretically studied by Lütkenhaus [32] and Inamori et al. [33], and a notable framework for safety analysis of actual devices was established by Gottesman et al. [34]. Various protocols were also announced to deal with this issue. Relevant protocols include the decoy state [35–37], the Scarani–Acín–Ribordy–Gisin protocol [38], measurement device-independent (MDI) [39,40] and device-independent [41–43] protocols. For a more basic principle of QKD, we refer to two recent reviews: Xu et al. [44], who introduce the security of QKD with realistic device, and Pirandola et al. [45], who provide a general introduction and a comprehensive description of advances of QKD.

1.3. Focus and Outline of This Review

QKD has gradually matured after development over more than 30 years. The farthest distance of QKD via optical fiber link has exceeded 800 km [46]. Through quantum satellites, intercontinental QKD over one thousand kilometers has been achieved [47–49]. Commercial QKD systems have been already available on shelves. Some quantum networks have begun to build up, and relevant researches have been carried out [50,51].

However, there are still many challenges for large-scale QKD applications. In particular, there is a wide gap between existing QKD systems and traditional optical communication in terms of cost or integration level. Taking advantages of low cost, miniaturization, and industrial compatibility, integrated photonics show great potential for further promotion of QKD systems. In this review, we mainly concentrate on the advances in integrated chip-based photonic QKD.

The first step toward the application of integrated QKD is to realize functional QKD devices based on integrated platforms. The encoding and decoding of quantum states (normally photonic quantum states) are typical processes of QKD, and we summarize relative integrated devices in Table 1. In the past few decades, several integrated photon sources for QKD, including single-photon sources, weak coherent sources and entangled-photon sources, have been investigated, and their studies are listed in Table 2. Research of integrated quantum photonic detectors are collected in Table 3.

With the development of critical integrated devices, the principal verifications of QKD based on integrated platforms are gradually realized. Qubit-based QKD is the most mature QKD scheme, and related studies based on integrated systems are summarized in Table 4. We also pay attention to the applications of integration technology in some advanced QKD protocols, such as MDI-QKDs, which can be immune to all attacks on detectors. Relevant literature is summarized in Table 5. Furthermore, security analyses and CV-QKD and HD-QKD demonstrations based on integrated chips are collected in Table 6.

The outline of this review is as follows. In Section 2, we introduce the different integrated platforms for quantum photonics. In Section 3, the basic architecture of integrated QKD devices and implementations are discussed. In Section 4, we review the QKD demonstrations based on integrated platforms. In the last section, we provide some suggestions for future research.

Integration technology has an important impact not only on QKDs, but also on quantum computing and quantum information processing. Relevant studies include early reviews of advances in integrated quantum photonics [52,53] and silicon quantum photonics [54]. A list of reviews related to integrated quantum photonics is presented in Table 7.

Table 1. QKD systems with integrated encoding and decoding modules.

Reference	Platform	Encoding Way	Protocol	Encoding	Decoding	Notes
[55]	Si	Time bin	BB84	✔	✔	98% interference visibility
[56]	Si	Time bin	BB84	✔	✔	Interference visibility is 80% at 150 km
[57]	Si	Time bin	BB84	✔	✔	The lowest bit error rate is 0.7%
[58]	Si	Time bin	BB84	✔	✔	Silicon-based AMZI
[59]	Si	Time bin	BB84	✔	✔	Sifted key rate 2.4 kbps
[60]	Si	Time bin	BB84	✔	✔	45 km, WDM system
[61]	Si	Time bin	BB84	✔	✔	Stable WDM system for more than 30 days
[62]	Si	Polarization	BB84	✔	✔	Polarization extinction ratio greater than 20 dB
[63]	Si	Time bin	BB84	✔	✔	98.38% interference visibility
[64]	Si	Time bin	BB84	✔	✔	98.38% interference visibility
[65]	Si	Time bin	BB84	✔	✔	98.72% interference visibility
[66]	Si	Time bin	BB84	✔	✔	96% interference visibility
[67]	Si	Time bin	BB84	✘	✔	Non-blocking matrix switch
[68]	Si	Time bin	DPS	✘	✔	95.8% interference visibility
[69]	Si	Time bin	BB84	✘	✔	95.8% interference visibility
[70]	SiO_2	Polarization	BB84	✘	✔	Polarization extinction ratio 16 dB
[71]	SiO_2	Polarization	BB84	✘	✔	sifted key rate of 415 kbps
[72]	FLDW	Polarization	MDI-QKD	✘	✔	Bell state analyzer
[73]	Si	Time bin	BB84	✘	✔	Complementary decoding system
[74]	Si	Time bin	BB84	✘	✔	Low bit error rate AMZI
[75]	Si	Time bin	BB84	✘	✔	99% interference visibility
[76]	Si	Time bin	BB84	✘	✔	98.6% Interference visibility
[77]	$LiNbO_3$ Si	Time bin	BB84	✘	✔	Extinction ratios are 18.65 dB and 15.46 dB
[78]	Si	OAM	HD-QKD	✔	✘	Generating three OAM modes
[79]	Si	Polarization	-	✔	✘	Polarization extinction ratio greater than 25 dB

Table 2. QKD systems with integrated sources.

Reference	Platform	Type	Notes
[80]	InP	weak coherent-state source	431 MHz HOM interference visibility is 46.5%± 0.8%
[81]	InP	coherent-state source	45 kHz side-mode suppression ratio of 54 dB
[82]	InP	weak coherent-state source	100 MHz HOM interference visibility is 46% ±2 %
[83]	Si	entangled photon pair source	431 MHz interference visibility is 92%
[84]	$LiNbO_3$ Si	entangled photon source	Interference visibility is 94%
[85]	Si	entangled photon source	High dimensional quantum information processing
[86]	Si	entangled photon source	Quantum information processing
[87]	Si	entangled photon source	Quantum information processing
[88]	hBN	single-photon source	Integrated room temperature single-photon source

Table 3. QKD systems with integrated detectors.

Reference	Platform	Encoding Way	Protocol	Source	Encoding	Decoding	Detection	Notes
[89]	Si_3N_4	Time bin	BB84	✘	✘	✔	✔	BB84 system
[90]	Si	Time bin	MDI-QKD	✘	✘	✔	✔	MDI-QKD system

Table 4. Qbit-based QKD of BB84, DPS and COW protocols based on integrated platforms.

Reference	Platform	Encoding Way	Protocol	Source	Encoding	Decoding	Detection	Clock Rate (Hz)	Distance or Loss	Key Rate (kbit/s)
[91]	Si	Time bin	BB84	✘	✔	✔	✘	1.25 G	45 km	81.7
[92]	Si	Time bin	BB84	✘	✔	✔	✘	1.25 G	14.5 dB	200
[93]	Si	Polarization	BB84	✘	✔	✔	✘	10 M	5 km	0.95
			DPS					1.72 G	20 km	565
[94]	InP SiO_xN_y	Time bin	BB84	✔	✔	✔	✘	560 M	20 km	345
			COW					860 M	20 km	311
[95]	Si	Polarization Time bin	BB84	✘	✔	✔	✘	1 G	20 km	329
	Si SiO_xN_y	Time bin	COW					1.72 G	20 km	916
[96]	Si	Polarization	BB84	✘	✔	✘	✘	625 M	43 km	157
[97]	Si	Time bin	BB84	✘	✔	✔	✘	100 M	20 km	85.7
[98]	Si	Time bin	BB84	✔	✔	✘	✘	1 G	100 km	270
			DPS					1 G	100 km	400
[99]	Si	Polarization	BB84	✘	✘	✔	✘	10 M	20 km	13.68
[100]	Si	Polarization	BB84	✘	✔	✘	✘	10 M	145 m	30
			DPS					2 G	14 dB	400
[101]	SiO_xN_y	Time bin	BB84	✘	✔	✘	✘	2 G	14 dB	500
			COW					2 G	14 dB	2500
[89]	Si_3N_4	Time bin	BB84	✘	✘	✔	✔	2.6 G	2.5 dB	1500
[102]	Si InP	Time bin	BB84	✔	✔	✔	✘	1 G	25 km	235
[103]	Si	Polarization	BB84	✘	✔	✔	✘	2 G	20 km	868
[104]	Si	Polarization	BB84	✘	✔	✘	✘	312.5 M	100 km	42.7
[105]	Si	Time bin	BB84	✘	✔	✔	✘	1.25 G	50 km	1340
[106]	Si	Time bin	DPS	✘	✘	✔	✘	1 G	20 km	3.076
[107]	Si	Time bin	DPS	✘	✘	✔	✘	1 G	17.6 km	120

Table 5. MDI-QKDs based on integrated systems.

Reference	Platform	Encoding Way	Protocol	Source	Encoding	Decoding	Detection	Clock Rate (Hz)	Distance or Loss	Key Rate (kbit/s)
[108]	Si	Polarization	MDI-QKD	✘	✔	✔	✘	0.5 M	50 km	1.46×10^{-3}
[109]	InP	Time bin	MDI-QKD	✔	✔	✘	✘	250 M	100 km	1
[110]	Si	Polarization	MDI-QKD	✘	✔	✘	✘	1.25 G	36 dB	31×10^{-3}
[111]	Si	Polarization	MDI-QKD	✘	✔	✘	✘	1.25 G	24 dB	137×10^{-3}
[90]	Si	Time bin	MDI-QKD	✘	✘	✔	✔	125 M	39.5 dB	34×10^{-3}

Table 6. Other integrated QKDs.

Reference	Platform	Encoding Way	Protocol	Source	Encoding	Decoding	Detection	Clock Rate (Hz)	Distance or Loss	Key Rate (kbit/s)	Notes
[112]	Si	path	HD-QKD	✘	✔	✔	✘	5 k	4 dB	7.5×10^{-3}	-
[113]	Si	Gaussian-modulated	CV-QKD	✘	✔	✔	✔	250 M	2 m	250	-
[114]	Si	Gaussian-modulated	CV-QKD	✘	✔	✘	✘	-	-	-	Security analysis
[115]	Si	Polarization	MDI-QKD	✘	✔	✘	✘	-	-	-	Security analysis
[116]	Si	Polarization	BB84	✘	✔	✔	✔	-	-	-	Security analysis

Table 7. Reviews of integrated quantum photonics.

Reference	Notes
[117]	Quantum communication
[54]	Silicon quantum photonics
[118]	Quantum photonic network
[53]	Photonic quantum information processing
[119]	Photonic quantum information processing
[52]	Photonic quantum information processing
[120]	Hybrid integrated quantum photonic circuits
[121]	Quantum entanglement on photonic chips
[122]	Femtosecond laser technology
[123]	Integrated photon technology
[124]	Silicon based quantum optical system devices
[125]	Direct phase modulated laser
[126]	Development, challenges, and directions of integrated quantum optics
[127]	Quantum communication and Quantum networks
[128]	Integrated photon-pair sources with nonlinear optics
[129]	Status, development and challenges of integrated quantum optics
[130]	Semiconductor quantum dot source and Quantum communication

2. Integrated Quantum Photonic Technology

The wide deployment of QKD requires a low-cost, robust, and miniature system. Integrated photonics provides potential for QKD devices in terms of complexity, robustness, and scalability. Many physical platforms have been studied for quantum implementations, and quantum photonic technology has raced ahead because of its relative simplicity in generation, manipulation, and detection. Serving as the carrier for quantum information, photons own the strength that can be inherently encoded in diverse degrees of freedom, involving temporal [131,132], frequency [133,134], path [85,135], and orbital angular momentum (OAM) [136,137]. In addition, multiple degrees of freedom of a photon can be used simultaneously [138]. To date, a series of photonic quantum implementations has been realized. As quantum systems scale up, the requirements for their stability, manufacturability, and programmability will be increasingly higher, and the miniaturization and chip-level integration of optical quantum implements are crucial to expand the complexity and functionality of quantum systems.

A range of photonic integration platforms has been investigated for quantum applications, including silica-on-insulator [139–141], silicon-on-insulator [142–146], silicon nitride (Si_3N_4) [147–150], silicon carbide [151], silicon oxynitride (SiO_xN_y) [95,133], lithium niobate (LN) [152–154], gallium arsenide (GaAs) [155–157], indium phosphide (InP) [95,158], and diamond [159], etc. Although the thickness of waveguides fabricated on silica-on-insulator is usually in the order of several microns whereas that of structures on silicon-on-insulator comes down to an order of hundreds of nanometers, both platforms can be referred to as planar lightwave circuits (PLCs) because the thickness of waveguides on a single chip is basically the same; that is, waveguides are in the same plane. Components created in the material platforms introduced above are typically 2D structures, whereas 3D photonic circuits can be integrated into a femtosecond laser direct written (FLDW) platform [160–163] because of the characteristics of fabrication processes. Different integrated platforms have their own superiorities. For instance, one prominent optical integration platform is nanostructures on silicon (Si) substrates. It has been used to realize various quantum facilities, including but not limited to the generation, detection, or manipulation of single-photon and high-dimensional entangled states [85], as well as some functions in chip-based quantum communication [94,110,113,164,165]. Another photonic integration standout is the FLDW platform. It has the typical advantage of arbitrary 3D circuit geometries in that it can be prepared by using the femtosecond laser direct writing technique. Many quantum tasks, such as 2D quantum walk [162] or homomorphic encryption [163], have been accomplished in this platform. The propagation loss of structures fabricated in Si_3N_4 platform

is ultralow [150]. LN is an arising and flexible integrated platform for entangled photon sources [152,153], superconducting detectors [154], and high-speed modulators [166,167]. In addition to LN [153], GaAs [157] and InP [95] also exhibit obvious electro-optic characteristics, allowing fast processing of single photons.

3. QKD Implementation

A QKD implementation consists of three parts: source, channel and detection, and different encoding or decoding schemes are embodied in these three parts. There are normally two types of channels in practical applications: free space and optical fibers. Theoretically, the safety of the system does not rely on the physical implementation of quantum channels. Technically, metropolitan QKD can take advantage of existing channels and associated infrastructures. Thus, most of the research on integrated QKD focused on sources, modulators, and circuits. Here, we mainly pay attention to the functional devices of source, detection, encoding, and decoding.

3.1. Encoding and Decoding

For qubit-based QKDs, quantum information is usually encoded in two orthogonal quantum states and their relative phases—for example, the use of orthogonal polarizations or distinct time bins. Both encoding methods allow robust quantum communication between chips via optical fibers. From an experimental point of view, polarization encoding means modulating the phase of two orthogonal modes of one pulse, whereas time-bin encoding means dividing one pulse into two bits with different time slots and modulating the phases of front and rear bits. The encoding and decoding processes of the polarization scheme and associated devices are relatively simple. However, there will be phase changes between two modes at the receiver due to imperfections of infrastructure like birefringence of fibers. By using time-bin encoding, phases of bits at different time slots are modulated; thus, time delay is needed at the decoder to obtain synchronous phase superposition. This time delay is easily disturbed by environmental factors such as temperature and becomes inaccurate, so the requirements for experimental conditions and devices used in decoding process are relatively higher.

In Table 1, we summarize a list of works of integrated devices for QKD encoding and decoding. An early work of integrated time-bin encoding and decoding implementation [55] was reported by researchers from the Institute of Semiconductors, Chinese Academy of Sciences (IOS-CAS). An asymmetric Mach–Zehnder interferometer (AMZI) was integrated on Si substrate, and its interference visibility was higher than 98%. As the technology developed, more components were fabricated on Si chips, and the interference visibilities of devices were gradually improved [58,63–65,74]. A new work reported a decoding chip, which was composed of two AMZIs, three variable optical beam splitters, and four variable directional couplers. The corresponding interference visibility reached 98.6% under temperature control [76]. Long-distance tests with integrated devices for time-bin encryption and decryption were also carried out. For example, time-bin coding devices made of PLCs were used in a QKD field trial, and the quantum bit error rate (QBER) was 2.8% after 97 km transmission [59]. Integrated AMZIs were also used for single-photon interference, and its fringe visibility was more than 80% after 150 km propagation [56]. In addition, a series of integrated components for time-bin encryption or decryption were achieved [57,66,68,69,73,77], including wavelength division multiplexing systems [60,61], matrix switch [67], and polarization-insensitive interferometers [75], etc.

Polarization encoding and decoding devices were also integrated based on different platforms. For instance, a transceiver with a polarization extinction ratio greater than 20 dB was fabricated onto Si substrate [62]. Si-based devices included a dynamic polarization controller, the dynamic polarization extinction ratio of which was greater than 25 dB [79]. Polarization beam splitters based on silica PLC platforms were used for free-space QKD applications [70,71]. Ten Bell-state analyzers were integrated into a FLDW photonic chip for future MDI-QKD applications [72].

For a qudit-based QKD, quantum information is encoded into d (d > 2) orthogonal states. OAM [78], which contains a large Hilbert space, is a typical choice for the integration of qudit-based QKD encoding. To the best of our knowledge, a path-encoding and path-decoding system is also realized for integrated qudit-based QKD [112]. Other coding methods, such as multiple time bin, are also applied to the macroqudit-based QKD and are expected to develop toward integration systems.

3.2. Photon Source

In the process of quantum coding, a QKD scheme usually needs to be associated with a quantum source. Here, we mainly outline the quantum photon sources used in QKDs (Table 2) and divide them into three categories: single-photon sources, weak coherent sources, and entangled-photon sources.

Theoretically, each optical pulse emitted by an ideal single-photon source contains only one single photon. But in practical application, it is very difficult to realize devices that can truly generate a single photon per pulse on demand. A promising study was an ultrabright solid-state single-photon source that was reported recently [88]. This photon source was achieved by integrating an atomic defect in hexagonal boron nitride (hBN) associated with a solid immersion lens; it could generate over ten million photons per second at room temperature.

In practical QKD applications, weak coherent sources, which can be easily obtained by attenuating laser emissions, are widely used to approximate single-photon sources. Weak coherent sources were mainly integrated onto InP substrates. One research study showed the visibility of Hong–Ou–Mandel interference between weak coherent states, which were generated by two independent InP transmitters at 431 MHz, was about 46% [80]. A similar result was also observed on two independent III-V lasers at 100 MHz [82]. A recent study [81] reported a Bragg reflection laser that exhibited a minimum inherent linewidth of 10 kHz and an experimental linewidth of 45 kHz by using a delayed self-heterodyne method. The laser operated under single-mode suppression, and the side mode rejection ratio was 54 dB.

Entangled-photon pairs can be generated based on nonlinear optics, i.e., spontaneous parametric downconversion (SPDC) [84] and spontaneous four-wave mixing (SFWM). By using SFWM, photon pairs could be created in microring resonators [83,86] or spiral structures [85,87]. The entangled-photon source (94% visibilities, 3% quantum error rate, 110 bit/s sifted key rate) based on SPDC was integrated into an LN-Si hybrid platform, whereas SFWM-based entangled-photon sources were mainly fabricated on Si substrates. A newer example [85] that demonstrated an Si chip containing more than 550 photonic components and including 16 identical photon-pair sources provided candidates for HD QKDs.

3.3. Detection

In the QKD schemes, the receivers use single-photon detectors to read out the quantum information prepared by senders. Single-photon detectors' technologies involve avalanche photodiodes (APDs) [168–170] and superconducting nanowire single-photon detectors (SNSPDs) [171–174]. As in the case with APDs, traditional SNSPDs are difficult to integrate with other photonic circuits. Hence, the single photons are typically coupled out of the photonic circuit chip into a fiber before being coupled into single-photon detectors. Recently, the development of waveguide-integrated SNSPDs [175] provide a way to integrate full photonic circuity for a QKD receiver. Table 3 lists the QKD systems containing integrated waveguide SNSPDs. In 2011, Si-waveguide SNSPDs were used in the first optimal Bell-state measurement of time bin-encoded qubits produced by two independent lasers [90] and paved the way for QKD networks with untrusted relays. Si_3N_4-waveguides SNSPDs were used in a QKD experiment at 2.6 GHz clock rate [89]. The dead time of the SNSPDs was lower than 20 ns, and the dark-count rate was lower than 20 Hz.

4. QKD Demonstration

In the section above, we mainly reviewed the functional verification of basic integrated devices for QKD implementation. However, a complete QKD scheme also needs to conduct data acquisition after random modulation, and to estimate the key rate according to the results of data acquisition. Post-processing, such as privacy amplification, error correction, verification, and authentication are also required. In this section, we will review research that completed QKD demonstrations.

4.1. Qubit-Based QKD

In Table 4, we summarize works of integrated qubit-based QKDs in chronological order. The first Si photonic integrated circuit transmitter was reported for polarization-encoded QKD [93]. In a 1.3×3 mm^2 die area, a pulse generator, a microring intensity modulator, a variable optical attenuator (VOA), and a polarization controller were integrated together (Figure 1a). The QKD experiment was demonstrated over a 5-km fiber link. Its estimated asymptotic secret key rate (EASKR) reached 0.95 kbps at a 10 MHz clock-rate. This work illustrates the potential of manufacturing low-cost, wafer-scale quantum components on an Si photonic platform. Thereafter, another Si optical integrated system was demonstrated by Sibson et al. [94]. This system consisted of a high-speed transmitter and the corresponding decoder. The fast modulation of quantum states was achieved by combining a thermally tuned phase shifter with a carrier-dispersive phase shifter. Three demonstrations were realized: time bin-encoded BB84 (Figure 1d), polarization-encoded BB84 (1 GHz clock rate, 329 kbps EASKR) (Figure 1c), and pulse modulation for COW QKD (1.72 GHz clock rate, 916 kbps EASKR) (Figure 1b) on an optical fiber network over a 20-km distance. The clock rate of the latter Si integrated system is much higher than that of the former one, whereas more components, i.e., the whole QKD emitter, were fabricated into the former system.

A differential phase shift (DPS) QKD demonstration was carried out with a PLC Mach–Zehnder interferometer. Polarization-insensitive operation at 1 GHz was achieved with a 3076 bits/s key creation rate and a 5.0% QBER [106]. A field test of DPS QKD was performed on a 17.6-km fiber network, and stable operation for six hours was realized with a 120-kbps sifted key rate and a 3.14% average QBER [107]. In a field trial of the Tokyo QKD network, a 2×2 AMZI made of PLC was used to help realization of the first secure TV conference over a 45-km distance [91]. The first field test of high-speed polarization-encoded QKD was demonstrated by Bunandar et al. [96], and the secret key rate reached was 1.039 Mbps on 103.6-m deployed fiber links and 157 kbps on 43-km deployed fiber links.

The Si-based integrated chip provided a phase-stable platform for high-speed QKD. Other qubit-based QKD demonstrations using Si-based implementations include works carried out by Huawei [97], the Toshiba Cambridge Institute [98], Sun Yat-sen University [99], the University of Padua [100], IOS-CAS [103,105] and the University of Science and Technology of China [104,105].

An Si-based integrated platform has been used to perform QKD demonstrations, but it usually requires discrete optics, external laser sources, and intensity modulators. A hybrid system with the InP integration platform can meet these requirements. For example, an entirely standalone system used for quantum random number generation and QKD at GHz clock rate was achieved by using a hybrid system [102]. In this system, the high-bandwidth photon sources, electro-absorption modulators and detectors were monolithically integrated on an InP chip as transmitter and a quantum random number generator, whereas the receiver part was fabricated on an Si-based substrate for low propagation loss. Complete electronic control and a post-processing program were also equipped. By using this system, a long-term stable QKD was demonstrated.

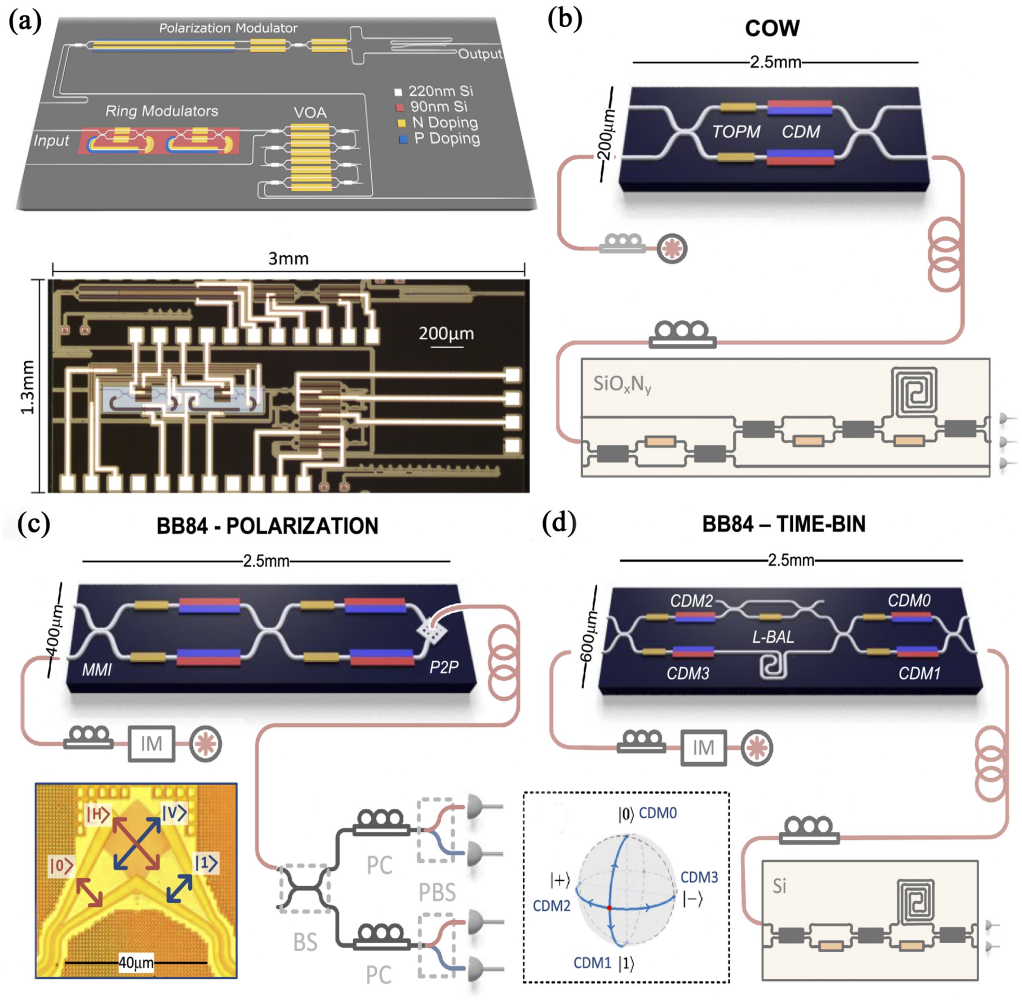

Figure 1. Integrated photonic chips for qubit-based QKDs. (**a**) Schematic and optical micrograph of the first Si-based integrated transmitter for polarization-encoded QKD. In a 1.3 mm × 3 mm die area, a pulse generator, a microring intensity modulator, a VOA, and a polarization controller were integrated together. (**b**) Chip-to-chip QKD for realization of COW. Beam splitters, thermo-optic phase modulators (TOPMs) and carrier-depletion modulators (CDMs) are integrated in an Si chip, which is used for the encoding of quantum information in path, or pulse modulation. (**c**) Polarization-encoded BB84. Two multimode interferences (MMIs) act as the two paths of an MZI, combining with a 2D grating coupler, for the conversion from path-encoded information to polarization-encoded information (P2P). (**d**) Time bin-encoded BB84. Four CDMs used for fast modulation. L-BAL stands for loss-balancing. Panels reproduced from: (**a**) [93]; (**d**) [94] under a Creative Commons licence (https://creativecommons.org/licenses/by/4.0/accessed date: 29 July 2022).

Another hybrid system (Figure 2) included a 2 × 6 mm^2 integrated InP transmitter and a 2 × 32 mm^2 SiO_xN_y photonic receiver circuit [95]. With the exception of detectors and link controllers, all devices were integrated into chips. Three time bin-modulated QKD demonstrations were realized based on this system: BB84 (560 MHz clock rate, 345 kbps estimated secret key rate), COW (0.86 GHz clock rate, 311 kbps estimated secret key rate) and DPS (1.72 GHz clock rate, 565 kbps estimated secret key rate), by using an attenuation equal to 20-km fiber. The performance of this system could be comparable with the most advanced optical fiber QKD system.

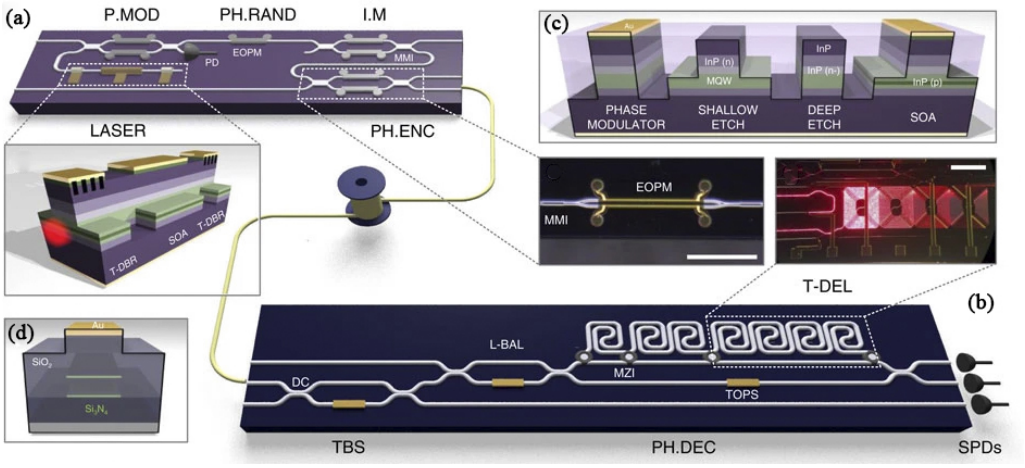

Figure 2. A hybrid system including an integrated InP transmitter and an SiO_xN_y receiver. The system is used for reconfigurable, multi-protocol QKD. (**a**) The InP transmitter chip. (**b**) The SiO_xN_y receiver circuit. (**c**) Cross-section of the InP deep-etch waveguides. (**d**) Cross-section of the SiO_xN_y Triplex waveguides. Panels reproduced from [95] under a Creative Commons licence (https://creativecommons.org/licenses/by/4.0/ accessed date: 29 July 2022).

The SiO_xN_y integrated receiver used in the investigations reported by Sibson et al. [94,95] was composed of waveguides that were fabricated by depositing and etching alternating layers of silica and Si_3N_4 (Figure 2d). Compared to Si waveguides, SiO_xN_y waveguide structures exhibited high index contrast but low propagation loss, as well as low coupling loss with fibers. Compared to silica PLC [92], SiO_xN_y circuits allow for more complexity. Another SiO_xN_y integrated receiver was used for QKD demonstrations of BB84, DPS, and COW schemes, and their secret key rates were 500 kbps, 400 kbps, and 2500 kbps, respectively, at 2 GHz clock rate [101].

An integrated receiver circuit was created on the Si_3N_4 photonic platform [89], which consisted of 325 nm Si_3N_4 on 3300 nm silica on an Si substrate. This low-loss chip featured all necessary components, including high-performance single-photon detectors, and it was used for a time-bin BB84 demonstration with a 1500 kbps key rate at 2.6 GHz over a 2.5 dB-loss channel.

4.2. MDI-QKD

MDI-QKD is a functional scheme that completely closes all security loopholes in the detection of physical implementations, thereby ensuring the security of communication through untrusted nodes. It has outstanding advantages. For example, MDI-QKD is easy to implement [176]. It also allows cost-effective multiuser-integrated systems, in which users only pay for low-cost transmitter chips while sharing the expensive devices (e.g., SNSPDs) among many users in a public, untrusted relay. Moreover, MDI-QKD supports longer transmission distance compared to traditional QKD systems.

Table 5 lists demonstrations of MDI-QKD based on integrated photonic platforms.

Wei et al. [110] first performed a complete demonstration of 1.25 GHz polarization-encoding MDI-QKD by using an Si-based integrated chip (Figure 3). A high distill finite-key secret rate of 31 bps was achieved over a 36-dB loss channel and a 497-bps key rate was obtained over 140-km commercial fiber spools. To the best of our knowledge, this study was the first GHz MDI-QKD with random modulations and represented a crucial step toward quantum communication with untrusted relays. The security of this GHz system against Trojan horse attacks was verified later, and a 137-bps secret key rate over a 24-dB channel loss was achieved [111].

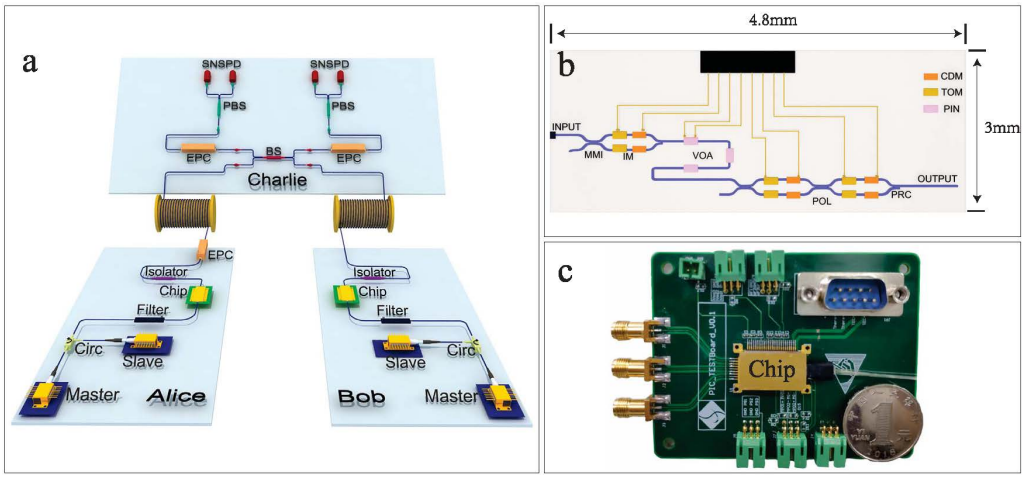

Figure 3. An example of Si-chip-based photonic MDI-QKD system. (**a**) Experimental setup. (**b**) The schematic of the Si chip, in which multimode interference (MMI) couplers, thermo-optics modulators (TOMs), carrier-depletion modulators (CDMs), and a polarization rotator combiner (PRC) are integrated. (**c**) Image of the packaged chip soldered to a compact control board. Panels reused from Ref. [110].

A proof-of-concept integrated MDI-QKD system was announced by Cao et al. [108]. This system included two Si-based integrated transmitter chips, which operated at 0.5 MHz, and a server chip. Polarization-encoded weak coherent states could be produced with extinction ratios over 20 dB, which promised low-error MDI-QKD. In the proof-of-concept experiment, the system showed a key rate of 1.46 bps over a distance corresponding to 50-km fiber.

The first integrated relay server for MDI-QKD was demonstrated by using a heterogeneous superconducting Si photonic chip [90]. Taking advantage of the high-speed response of superconducting detectors, the optimal Bell-state measurement for time-bin qubits was performed for the first time. Combined with time-multiplexing technology, a secret key rate of 6.166 kbps at 125 MHz was realized over a 24-dB loss channel. This result was comparable to the state-of-the-art MDI-QKD experimental outcomes with a GHz clock rate. Another time bin-encoding MDI-QKD demonstration was performed on a system containing an InP chip, which allowed mass integration of cost-effective devices. Entirely on-chip components were used to prepare high-fidelity 250-MHz clocked weak coherent states. The demonstration showed a 1-kbps estimated secret key rate over a 100-km emulated fiber link, and the QBER was lower than 0.5% [109].

4.3. Other Integrated QKDs

There are a few studies related to qudit-based QKD, CV-QKD, and QKD security analyses, so we sorted them into the same table (Table 6).

Because qudit-based QKDs are developed in high-dimensional Hilbert spaces, they are also referred to as high-dimensional (HD) QKDs. Compared to qubit-based QKDs, qudit-based QKDs have better error tolerance and a higher quantum key rate per particle. However, qudit-based QKDs are ordinarily hard to implement in practice due to the difficulty in preparing high-fidelity qudit states. There are two noticeable exceptions called the Chau15 scheme [26] and the round-robin differential phase-shift (RRDPS) scheme [31], which were proposed recently. A qudit-based QKD was proposed and experimentally demonstrated based on space division multiplexing in multi-core fiber by using Si-based integrated path-encoded chips [112]. The use of the multi-core fiber enabled an efficient method for HD quantum state generation at a 5-kHz clock rate. Si-based chips allow stable manipulation of HD quantum states. Three mutually unbiased results were realized in a four-dimensional Hilbert space. A stable quantum bit error rate below coherent attack

and individual attack limits was obtained. In an actual decoy, four-dimensional BB84 experiment, the calculated key rate is 7.5 bps over the 4-dB loss channel.

In CV-QKD, the secret keys are encrypted in quadratures of the quantized electromagnetic field and decrypted by coherent detections. Coherent detection is compatible with existing communication infrastructures. Furthermore, it requires no cooling, and its detection efficiency is quite high. Thus, coherent detection becomes a potential application to realize practical quantum cryptography [177]. CV-QKDs can be divided into different classifications according to whether the detection methods are homodyne [178] or heterodyne detections [179], and whether the modulation schemes are Gaussian [180] or discrete modulations [181] etc. An experimental verification of CV-QKD was performed based on an Si photonic chip, in which all necessary components were integrated except the photon source [113]. This chip implemented Gaussian-modulated coherent state and was used for CV-QKD demonstration over a 2-m fiber. The resulting key rate was 0.25 Mbps. The feasibility of long-distance CV-QKD was also simulatively verified.

To date, only some theoretical models of QKD systems based on specific assumptions can be proven to have unconditional security. In fact, there are always various threats in the practical applications due to imperfections in the source [182–184], modulation [185,186], and detection [187–190]. In order to apply the unconditional security proof of the theoretical model to the actual QKD systems, it is necessary to build the theoretical model based on assumptions that can be verified by experiments and further develop corresponding tests meant to verify these assumptions—that is, security analyses, which include security definitions, implementation assumptions, and diverse security proofs. These issues are well studied for a bulk optic system [191–197]. The security analyses are also crucial for the chip-based QKD at a starting state. Here, we review some security analyses performed on integrated photonic QKD systems.

Although many QKD schemes have been demonstrated on integrated photonic chips, polarization-dependent loss in state preparation has not been considered in the key-rate estimation process. One recent study [116] illustrated that a large amount of polarization-dependent loss existed in realistic Si-based integrated state-preparation devices and might compromise system security. Then a decoy-state BB84 QKD experiment that took polarization-dependent loss into account was carried out, and a rigorous finite-key security bound was obtained over a fiber link up to 75 km. A security analysis of influence caused by carrier fluctuations combined the plasma dispersion effect and was performed on an Si-based integrated modulator used for CV-QKD [114]. Two preliminary defense strategies were proposed: the maximum carrier fluction deviation method and dynamic random carrier fluction calibration based on the deep neural network. The finite-key security of BB84 and MDI-QKD was analyzed based on an Si-integrated chip with information leakage out of polarization modulators and intensity modulators. With a 232-dB isolation, the MDI-QKD system was still able to resist the Trojan horse attack [115].

5. Conclusions and Outlook

In this review, we first introduced a basic QKD background (Section 1) and the development of integrated platforms applied to quantum photonics (Section 2). Then the performance of integrated quantum devices (Section 3) and a series of experimental QKD verifications based on photonic integrated chips (Section 4) were discussed.

Combined with various integration technologies, QKD systems will scale up quickly and promise more complexity and functionality. Here, we provide several suggestions for the focus of further researches.

1. Security analyses: The unconditional security of QKD is based on the hypothesis that the practical system model is consistent with the theoretical model used in the security proof. In fact, there are ineluctable differences between theoretical and practical system models that lead to security vulnerabilities in the QKD system. See reference [198] for a short overview of this topic. For integrated photonic QKD systems, further

security analyses, including calibrations or tests of whether the chips meet the safety assumptions and designs of secure testable systems, are still necessary.
2. Higher-level integrations of quantum photonic systems: We have described some QKD photonic chips in this review, and one can see that there is not a complete integrated system. In the future, complete integrated systems should be realized with the development of hybrid integration technologies.
3. Demonstrations of advanced QKD protocols: Previous studies of QKD demonstrations with integrated photonic chips were mostly based on classic protocols like BB84 or MDI. In the future, we should pay attention to combinations of integration technologies and cutting-edge QKD protocols, such as the recently proposed twin-field QKD [199,200], which can break through the PLOB bound [201], as well as its derivative protocols like phase-matching QKD [202], sending-or-not-sending [203], and no-phase-postelection protocols [204].

Author Contributions: Investigation, Q.L., Y.D. and Z.Z. (Zhengeng Zhao); data curation, Q.L., Y.D., Z.Z. (Zhengeng Zhao) and Y.H.; writing—original draft preparation, Q.L., Y.D. and Z.Z. (Zhengeng Zhao); writing—review and editing, Q.L., M.G. and K.W.; supervision, Q.L., K.W., M.G. and Z.Z. (Zhenrong Zhang); project administration, K.W.; funding acquisition, K.W. and Z.Z. (Zhenrong Zhang). All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the National Natural Science Foundation of China No. 62171144, the Guangxi Science Foundation (No. 2021GXNSFAA220011), and the Open Fund of IPOC (BUPT) (No. IPOC2021A02).

Data Availability Statement: Not applicable.

Acknowledgments: We thank Huihe Chen for helpful discussions.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Cyber-Attack Events. Available online: https://baijiahao.baidu.com/s?id=1721894808280657573&wfr=spider&for=pc (accessed on 28 July 2022).
2. Cyber-Attacks to Iranian Gas Station. Available online: https://baijiahao.baidu.com/s?id=1714920135423559999&wfr=spider&for=pc (accessed on 28 July 2022).
3. Attack to Florida Drinking Water Treatment Facilities. Available online: https://www.163.com/dy/article/H6EJJK8C05529LO2.html (accessed on 28 July 2022).
4. Arute, F.; Arya, K.; Babbush, R.; Bacon, D.; Bardin, J.C.; Barends, R.; Biswas, R.; Boixo, S.; Brandao, F.; Buell, D.A.; et al. Quantum supremacy using a programmable superconducting processor. *Nature* **2019**, *574*, 505–510. https://doi.org/10.1038/s41586-019-1666-5.
5. Zhong, H.S.; Wang, H.; Deng, Y.H.; Chen, M.C.; Peng, L.C.; Luo, Y.H.; Qin, J.; Wu, D.; Ding, X.; Hu, Y.; et al. Quantum computational advantage using photons. *Science* **2020**, *370*, 1460–1463. https://doi.org/10.1126/science.abe8770.
6. Wu, Y.; Bao, W.S.; Cao, S.; Chen, F.; Chen, M.C.; Chen, X.; Chung, T.H.; Deng, H.; Du, Y.; Fan, D.; et al. Strong Quantum Computational Advantage Using a Superconducting Quantum Processor. *Phys. Rev. Lett.* **2021**, *127*, 180501. https://doi.org/10.1103/PhysRevLett.127.180501.
7. Zhong, H.S.; Deng, Y.H.; Qin, J.; Wang, H.; Chen, M.C.; Peng, L.C.; Luo, Y.H.; Wu, D.; Gong, S.Q.; Su, H.; et al. Phase-Programmable Gaussian Boson Sampling Using Stimulated Squeezed Light. *Phys. Rev. Lett.* **2021**, *127*, 180502. https://doi.org/10.1103/PhysRevLett.127.180502.
8. Deshpande, A.; Mehta, A.; Vincent, T.; Quesada, N.; Hinsche, M.; Ioannou, M.; Madsen, L.; Lavoie, J.; Qi, H.; Eisert, J.; et al. Quantum computational advantage via high-dimensional Gaussian boson sampling. *Sci. Adv.* **2022**, *8*, eabi7894. https://doi.org/doi:10.1126/sciadv.abi7894.
9. Bernstein, D.J., Introduction to post-quantum cryptography. In *Post-Quantum Cryptography*; Springer: Berlin/Heidelberg, Germany, 2009; pp. 1–14.
10. Long, G.L.; Liu, X.S. Theoretically efficient high-capacity quantum-key-distribution scheme. *Phys. Rev. A* **2002**, *65*, 032302. https://doi.org/10.1103/PhysRevA.65.032302.
11. Deng, F.G.; Long, G.L. Secure direct communication with a quantum one-time pad. *Phys. Rev. A* **2004**, *69*, 052319. https://doi.org/10.1103/PhysRevA.69.052319.
12. Liu, X.; Li, Z.; Luo, D.; Huang, C.; Ma, D.; Geng, M.; Wang, J.; Zhang, Z.; Wei, K. Practical decoy-state quantum secure direct communication. *Sci. China Phys. Mech. Astron.* **2021**, *64*, 120311. https://doi.org/10.1007/s11433-021-1775-4.

13. Sun, S.; Long, G. Deterministic secure quantum communication with practical devices. *Quant. Eng.* **2021**, *3*, e86. https://doi.org/10.1002/que2.86.
14. Sheng, Y.B.; Zhou, L.; Long, G.L. One-step quantum secure direct communication. *Sci. Bull.* **2022**, *67*, 367–374. https://doi.org/10.1016/j.scib.2021.11.002.
15. Qi, R.; Sun, Z.; Lin, Z.; Niu, P.; Hao, W.; Song, L.; Huang, Q.; Gao, J.; Yin, L.; Long, G.L. Implementation and security analysis of practical quantum secure direct communication. *Light Sci. Appl.* **2019**, *8*, 22. https://doi.org/10.1038/s41377-019-0132-3.
16. Pan, D.; Lin, Z.; Wu, J.; Zhang, H.; Sun, Z.; Ruan, D.; Yin, L.; Long, G.L. Experimental free-space quantum secure direct communication and its security analysis. *Photon. Res.* **2020**, *8*, 1522–1531. https://doi.org/10.1364/prj.388790.
17. Zhang, H.; Sun, Z.; Qi, R.; Yin, L.; Long, G.L.; Lu, J. Realization of quantum secure direct communication over 100 km fiber with time-bin and phase quantum states. *Light Sci. Appl.* **2022**, *11*, 83. https://doi.org/10.1038/s41377-022-00769-w.
18. Wang, X.; Sun, X.; Liu, Y.; Wang, W.; Kan, B.; Dong, P.; Zhao, L. Transmission of photonic polarization states from geosynchronous Earth orbit satellite to the ground. *Quant. Eng.* **2021**, *3*, e73. https://doi.org/10.1002/que2.73.
19. Bennett, C.H.; Brassard, G. An update on quantum cryptography. In Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques, Paris, France, 9–11 April 1984; Springer: Berlin/Heidelberg, Germany, 1984; pp. 475–480.
20. Lo, H.K.; Chau, H.F. Unconditional Security of Quantum Key Distribution over Arbitrarily Long Distances. *Science* **1999**, *283*, 2050–2056.
21. Bennett, C.H. Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett.* **1992**, *68*, 3121–3124. https://doi.org/10.1103/PhysRevLett.68.3121.
22. Inoue, K.; Waks, E.; Yamamoto, Y. Differential phase shift quantum key distribution. *Phys. Rev. Lett.* **2002**, *89*, 037902. https://doi.org/10.1103/PhysRevLett.89.037902.
23. Stucki, D.; Brunner, N.; Gisin, N.; Scarani, V.; Zbinden, H. Fast and simple one-way quantum key distribution. *Appl. Phys. Lett.* **2005**, *87*, 194108. https://doi.org/10.1063/1.2126792.
24. Ekert, A.K. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **1991**, *67*, 661–663. https://doi.org/10.1103/PhysRevLett.67.661.
25. Scarani, V.; Bechmann-Pasquinucci, H.; Cerf, N.J.; Dušek, M.; Lütkenhaus, N.; Peev, M. The security of practical quantum key distribution. *Rev. Mod. Phys.* **2009**, *81*, 1301–1350. https://doi.org/10.1103/RevModPhys.81.1301.
26. Chau, H.F. Quantum key distribution using qudits that each encode one bit of raw key. *Phys. Rev. A* **2015**, *92*, 062324. https://doi.org/10.1103/PhysRevA.92.062324.
27. Bechmann-Pasquinucci, H.; Peres, A. Quantum cryptography with 3-state systems. *Phys. Rev. Lett.* **2000**, *85*, 3313–3316. https://doi.org/10.1103/PhysRevLett.85.3313.
28. Bechmann-Pasquinucci, H.; Tittel, W. Quantum cryptography using larger alphabets. *Phys. Rev. A* **2000**, *61*, 062308. https://doi.org/10.1103/PhysRevA.61.062308.
29. Cerf, N.J.; Bourennane, M.; Karlsson, A.; Gisin, N. Security of quantum key distribution using d-level systems. *Phys. Rev. Lett.* **2002**, *88*, 127902. https://doi.org/10.1103/PhysRevLett.88.127902.
30. Chau, H.F. Unconditionally Secure Key Distribution in Higher Dimensions by Depolarization. *IEEE Trans. Inf. Theory* **2005**, *51*, 1451–1468. https://doi.org/10.1109/tit.2005.844076.
31. Sasaki, T.; Yamamoto, Y.; Koashi, M. Practical quantum key distribution protocol without monitoring signal disturbance. *Nature* **2014**, *509*, 475–478. https://doi.org/10.1038/nature13303.
32. Lütkenhaus, N. Security against individual attacks for realistic quantum key distribution. *Phys. Rev. A* **2000**, *61*, 052304. https://doi.org/10.1103/PhysRevA.61.052304.
33. Inamori, H.; Lütkenhaus, N.; Mayers, D. Unconditional security of practical quantum key distribution. *Eur. Phys. J. D* **2007**, *41*, 599–627. https://doi.org/10.1140/epjd/e2007-00010-4.
34. Gottesman, D.; Lo, H.K.; Lütkenhaus, N.; Preskill, J. Security of quantum key distribution with imperfect devices. *Quantum Inf. Comput.* **2004**, *4*, 325–360. https://doi.org/10.1109/ISIT.2004.1365172.
35. Hwang, W.Y. Quantum key distribution with high loss: toward global secure communication. *Phys. Rev. Lett.* **2003**, *91*, 057901. https://doi.org/10.1103/PhysRevLett.91.057901.
36. Lo, H.K.; Ma, X.; Chen, K. Decoy state quantum key distribution. *Phys. Rev. Lett.* **2005**, *94*, 230504. https://doi.org/10.1103/PhysRevLett.94.230504.
37. Wang, X.B. Beating the photon-number-splitting attack in practical quantum cryptography. *Phys. Rev. Lett.* **2005**, *94*, 230503. https://doi.org/10.1103/PhysRevLett.94.230503.
38. Scarani, V.; Acin, A.; Ribordy, G.; Gisin, N. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. *Phys. Rev. Lett.* **2004**, *92*, 057901. https://doi.org/10.1103/PhysRevLett.92.057901.
39. Lo, H.K.; Curty, M.; Qi, B. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **2012**, *108*, 130503. https://doi.org/10.1103/PhysRevLett.108.130503.
40. Braunstein, S.L.; Pirandola, S. Side-channel-free quantum key distribution. *Phys. Rev. Lett.* **2012**, *108*, 130502. https://doi.org/10.1103/PhysRevLett.108.130502.
41. Mayers, D.; Yao, A. Quantum cryptography with imperfect apparatus. In Proceedings of the 39th Annual Symposium on Foundations of Computer Science (Cat. No. 98CB36280), Palo Alto, CA, USA, 8–11 November 1998; pp. 503–509.

42. Barrett, J.; Hardy, L.; Kent, A. No signaling and quantum key distribution. *Phys. Rev. Lett.* **2005**, *95*, 010503. https://doi.org/10.1103/PhysRevLett.95.010503.
43. Acin, A.; Brunner, N.; Gisin, N.; Massar, S.; Pironio, S.; Scarani, V. Device-independent security of quantum cryptography against collective attacks. *Phys. Rev. Lett.* **2007**, *98*, 230501. https://doi.org/10.1103/PhysRevLett.98.230501.
44. Xu, F.; Ma, X.; Zhang, Q.; Lo, H.K.; Pan, J.W. Secure quantum key distribution with realistic devices. *Rev. Mod. Phys.* **2020**, *92*, 025002. https://doi.org/10.1103/RevModPhys.92.025002.
45. Pirandola, S.; Andersen, U.L.; Banchi, L.; Berta, M.; Bunandar, D.; Colbeck, R.; Englund, D.; Gehring, T.; Lupo, C.; Ottaviani, C.; et al. Advances in quantum cryptography. *Adv. Opt. Photonics* **2020**, *12*, 1012–1236. https://doi.org/10.1364/AOP.361502.
46. Wang, S.; Yin, Z.Q.; He, D.Y.; Chen, W.; Wang, R.Q.; Ye, P.; Zhou, Y.; Fan-Yuan, G.J.; Wang, F.X.; Chen, W.; et al. Twin-field quantum key distribution over 830-km fibre. *Nat. Photonics* **2022**, *16*, 154–161. https://doi.org/10.1038/s41566-021-00928-2.
47. Liao, S.K.; Cai, W.Q.; Liu, W.Y.; Zhang, L.; Li, Y.; Ren, J.G.; Yin, J.; Shen, Q.; Cao, Y.; Li, Z.P.; et al. Satellite-to-ground quantum key distribution. *Nature* **2017**, *549*, 43–47. https://doi.org/10.1038/nature23655.
48. Liao, S.K.; Cai, W.Q.; Handsteiner, J.; Liu, B.; Yin, J.; Zhang, L.; Rauch, D.; Fink, M.; Ren, J.G.; Liu, W.Y.; et al. Satellite-Relayed Intercontinental Quantum Network. *Phys. Rev. Lett.* **2018**, *120*, 030501. https://doi.org/10.1103/PhysRevLett.120.030501.
49. Yin, J.; Li, Y.H.; Liao, S.K.; Yang, M.; Cao, Y.; Zhang, L.; Ren, J.G.; Cai, W.Q.; Liu, W.Y.; Li, S.L.; et al. Entanglement-based secure quantum cryptography over 1,120 kilometres. *Nature* **2020**, *582*, 501–505. https://doi.org/10.1038/s41586-020-2401-y.
50. Dynes, J.F.; Wonfor, A.; Tam, W.W.S.; Sharpe, A.W.; Takahashi, R.; Lucamarini, M.; Plews, A.; Yuan, Z.L.; Dixon, A.R.; Cho, J.; et al. Cambridge quantum network. *NPJ Quantum Inf.* **2019**, *5*, 101. https://doi.org/10.1038/s41534-019-0221-4.
51. Chen, Y.A.; Zhang, Q.; Chen, T.Y.; Cai, W.Q.; Liao, S.K.; Zhang, J.; Chen, K.; Yin, J.; Ren, J.G.; Chen, Z.; et al. An integrated space-to-ground quantum communication network over 4,600 kilometres. *Nature* **2021**, *589*, 214–219. https://doi.org/10.1038/s41586-020-03093-8.
52. Wang, J.; Sciarrino, F.; Laing, A.; Thompson, M.G. Integrated photonic quantum technologies. *Nat. Photonics* **2020**, *14*, 273–284. https://doi.org/10.1038/s41566-019-0532-1.
53. Flamini, F.; Spagnolo, N.; Sciarrino, F. Photonic quantum information processing: A review. *Rep. Prog. Phys.* **2019**, *82*, 016001. https://doi.org/10.1088/1361-6633/aad5b2.
54. Silverstone, J.W.; Bonneau, D.; O'Brien, J.L.; Thompson, M.G. Silicon Quantum Photonics. *IEEE J. Sel. Top Quantum Electron.* **2016**, *22*, 390–402. https://doi.org/10.1109/jstqe.2016.2573218.
55. Nambu, Y.; Hatanaka, T.; Nakamura, K. Planar lightwave circuits for quantum cryptographic systems. *arXiv* **2003**, arXiv:quant-ph/0307074.
56. Kimura, T.; Nambu, Y.; Hatanaka, T.; Tomita, A.; Kosaka, H.; Nakamura, K. Single-photon Interference over 150 km Transmission Using Silica-based Integrated-optic Interferometers for Quantum Cryptography. *Jpn. J. Appl. Phys.* **2004**, *43*, L1217–L1219. https://doi.org/10.1143/jjap.43.L1217.
57. Yoshino, K.; Tanaka, A.; Nambu, Y.; Tajima, A.; Tomita, A. Dual-mode Time-bin Coding for Quantum Key Distribution Using Dual-drive Mach-Zehnder Modulator. In Proceedings of the 33rd European Conference and Exhibition of Optical Communication, Berlin, Germany, 16–20 September 2007; pp. 1–2. https://doi.org/10.1049/ic:20070342.
58. Nambu, Y.; Yoshino, K.; Tomita, A. Quantum encoder and decoder for practical quantum key distribution using a planar lightwave circuit. *J. Mod. Opt.* **2008**, *55*, 1953–1970. https://doi.org/10.1080/09500340801942414.
59. Tanaka, A.; Fujiwara, M.; Nam, S.W.; Nambu, Y.; Takahashi, S.; Maeda, W.; Yoshino, K.; Miki, S.; Baek, B.; Zhen, W.; et al. 97-km QKD field trial using PLC-based one-way interferometers, SSPDs and WDM synchronization. In Proceedings of the Optical Fiber Communication Conference/National Fiber Optic Engineers Conference, San Diego, CA, USA, 24–28 February 2008; OSA Technical Digest (CD); Optica Publishing Group: Washington, DC, USA, 2008; p. OWJ2. https://doi.org/10.1109/OFC.2008.4528716.
60. Yoshino, K.I.; Fujiwara, M.; Tanaka, A.; Takahashi, S.; Nambu, Y.; Tomita, A.; Miki, S.; Yamashita, T.; Wang, Z.; Sasaki, M.; et al. High-speed wavelength-division multiplexing quantum key distribution system. *Opt. Lett.* **2012**, *37*, 223–225. https://doi.org/10.1364/OL.37.000223.
61. Yoshino, K.i.; Ochi, T.; Fujiwara, M.; Sasaki, M.; Tajima, A. Maintenance-free operation of WDM quantum key distribution system through a field fiber over 30 days. *Opt. Express* **2013**, *21*, 31395–31401. https://doi.org/10.1364/OE.21.031395.
62. Cai, H.; Long, C.M.; DeRose, C.T.; Boynton, N.; Urayama, J.; Camacho, R.; Pomerene, A.; Starbuck, A.L.; Trotter, D.C.; Davids, P.S.; et al. Silicon photonic transceiver circuit for high-speed polarization-based discrete variable quantum key distribution. *Opt. Express* **2017**, *25*, 12282–12294. https://doi.org/10.1364/OE.25.012282.
63. Zhang, W.; Kadosawa, Y.; Tomita, A.; Ogawa, K.; Okamoto, A. State preparation robust to modulation signal degradation by use of a dual parallel modulator for high-speed BB84 quantum key distribution systems. *Opt. Express* **2020**, *28*, 13965–13977. https://doi.org/10.1364/OE.383175.
64. Ren, M.; Li, X.; Zhang, J.; Wang, L.; Wang, Y.; Wu, Y.; An, J. Single-photon interference using silica-based AMZI with phase modulation. *Opt. Laser Technol.* **2020**, *122*, 105837. https://doi.org/10.1016/j.optlastec.2019.105837.
65. Li, X.; Ren, M.; Zhang, J.; Wang, L.; Chen, W.; Wang, Y.; Yin, X.; Wu, Y.; An, J. Interference at the single-photon level based on silica photonics robust against channel disturbance. *Photonics Res.* **2021**, *9*, 222–228. https://doi.org/10.1364/prj.406123.
66. You, J.; Wang, Y.; Cui, P.; Liu, Q.; Wu, D.; Li, S.; Zhang, J.; An, J.; Han, Q. Practical quantum key distribution module based on planar lightwave circuit. *IEEE Photon. Technol. Lett.* **2022**, *34*, 529–532. https://doi.org/10.1109/lpt.2022.3170925.

67. Honjo, T.; Inoue, K.; Sahara, A.; Yamazaki, E.; Takahashi, H. Quantum key distribution experiment through a PLC matrix switch. *Opt. Commun.* **2006**, *263*, 120–123. https://doi.org/10.1016/j.optcom.2006.01.018.
68. Yuki, I.; Toshimori, H.; Kyo, I.; Hidehiko, K.; Yoshiki, N.; Osamu, T.; Masaki, A. Polarization independent DPS-QKD system using up-conversion detectors. In Proceedings of the 2008 Conference on Lasers and Electro-Optics and 2008 Conference on Quantum Electronics and Laser Science, San Jose, CA, USA, 4–9 May 2008; pp. 1–2. https://doi.org/10.1109/QELS.2008.4553246.
69. Fujiwara, M.; Toyoshima, M.; Sasaki, M.; Yoshino, K.; Nambu, Y.; Tomita, A. Performance of hybrid entanglement photon pair source for quantum key distribution. *Appl. Phys. Lett.* **2009**, *95*, 261103. https://doi.org/10.1063/1.3276559.
70. Choe, J.S.; Choi, B.S.; Ko, H.; Youn, C.J. Silica PLC-based Polarization Beam Splitter for 780 nm Free-Space Quantum Key Distribution Applications. In Proceedings of the Asia Communications and Photonics Conference, Wuhan, China, 2–5 November 2016; OSA Technical Digest (Online); Optica Publishing Group: Washington, DC, USA, 2016; p. AF2A.45. https://doi.org/10.1364/ACPC.2016.AF2A.45.
71. Choe, J.S.; Ko, H.; Choi, B.S.; Kim, K.J.; Youn, C.J. Silica Planar Lightwave Circuit Based Integrated 1×4 Polarization Beam Splitter Module for Free-Space BB84 Quantum Key Distribution. *IEEE Photon. J.* **2018**, *10*, 1–8. https://doi.org/10.1109/jphot.2017.2788638.
72. Wang, C.Y.; Gao, J.; Jiao, Z.Q.; Qiao, L.F.; Ren, R.J.; Feng, Z.; Chen, Y.; Yan, Z.Q.; Wang, Y.; Tang, H.; et al. Integrated measurement server for measurement-device-independent quantum key distribution network. *Opt. Express* **2019**, *27*, 5982–5989. https://doi.org/10.1364/OE.27.005982.
73. You, J.; Wang, Y.; An, J. Balanced pulses in two outputs of quantum photonic chip. *Optoelectron. Lett.* **2021**, *17*, 592–597. https://doi.org/10.1007/s11801-021-0203-6.
74. You, J.; Wang, Y.; An, J.M. Realization of simultaneous balanced multi-outputs for multi-protocols QKD decoding based on silica-based planar lightwave circuit. *Chin. Phys. B* **2021**, *30*, 080302. https://doi.org/10.1088/1674-1056/abe2ff.
75. Zhang, G.W.; Ding, Y.Y.; Chen, W.; Wang, F.X.; Ye, P.; Huang, G.Z.; Wang, S.; Yin, Z.Q.; An, J.M.; Guo, G.C.; et al. Polarization-insensitive interferometer based on a hybrid integrated planar light-wave circuit. *Photonics Res.* **2021**, *9*, 2176–2181. https://doi.org/10.1364/prj.432327.
76. You, J.; Wang, Y.; Han, Q.; An, J. Silica-silicon based planar lightwave circuit quantum key distribution decoding chip for multi-protocol. *Opt. Laser Technol.* **2022**, *145*, 107505. https://doi.org/10.1016/j.optlastec.2021.107505.
77. Li, X.; Wang, L.L.; Zhang, J.S.; Chen, W.; Wang, Y.; Wu, D.; An, J.M. Quantum key distribution transmitter chip based on hybrid-integration of silica and lithium niobates. *Chin. Phys. B* **2022**, *31*, 064212. https://doi.org/ARTN064212 10.1088/1674-1056/ac40fe.
78. Zahidy, M.; Liu, Y.; Cozzolino, D.; Ding, Y.; Morioka, T.; Oxenløwe, L.K.; Bacco, D. Photonic integrated chip enabling orbital angular momentum multiplexing for quantum communication. *Nanophotonics* **2022**, *11*, 821–827. https://doi.org/10.1515/nanoph-2021-0500.
79. Wang, X.Y.; Jia, Y.X.; Guo, X.B.; Liu, J.Q.; Wang, S.F.; Liu, W.Y.; Sun, F.Y.; Zou, J.; Li, Y.M. Silicon photonics integrated dynamic polarization controller. *Chin. Opt. Lett.* **2022**, *20*, 041301. https://doi.org/Artn 04130110.3788/Col202220.041301.
80. Semenenko, H.; Sibson, P.; Thompson, M.G.; Erven, C. Interference between independent photonic integrated devices for quantum key distribution. *Opt. Lett.* **2019**, *44*, 275–278. https://doi.org/10.1364/OL.44.000275.
81. Kumar, R.R.; Hansel, A.; Far Brusatori, M.; Nielsen, L.; Augustin, L.M.; Volet, N.; Heck, M.J.R. A 10-kHz intrinsic linewidth coupled extended-cavity DBR laser monolithically integrated on an InP platform. *Opt. Lett.* **2022**, *47*, 2346–2349. https://doi.org/10.1364/OL.454478.
82. Agnesi, C.; Da Lio, B.; Cozzolino, D.; Cardi, L.; Ben Bakir, B.; Hassan, K.; Della Frera, A.; Ruggeri, A.; Giudice, A.; Vallone, G.; et al. Hong-Ou-Mandel interference between independent III-V on silicon waveguide integrated lasers. *Opt. Lett.* **2019**, *44*, 271–274. https://doi.org/10.1364/OL.44.000271.
83. Wakabayashi, R.; Fujiwara, M.; Yoshino, K.i.; Nambu, Y.; Sasaki, M.; Aoki, T. Time-bin entangled photon pair generation from Si micro-ring resonator. *Opt. Express* **2015**, *23*, 1103–1113. https://doi.org/10.1364/OE.23.001103.
84. Arahira, S.; Murai, H.; Sasaki, H. Generation of highly stable WDM time-bin entanglement by cascaded sum-frequency generation and spontaneous parametric downconversion in a PPLN waveguide device. *Opt. Express* **2016**, *24*, 19581–19591. https://doi.org/10.1364/OE.24.019581.
85. Wang, J.; Paesani, S.; Ding, Y.; Santagati, R.; Skrzypczyk, P.; Salavrakos, A.; Tura, J.; Augusiak, R.; Mancinska, L.; Bacco, D.; et al. Multidimensional quantum entanglement with large-scale integrated optics. *Science* **2018**, *360*, 285–291. https://doi.org/10.1126/science.aar7053.
86. Silverstone, J.W.; Santagati, R.; Bonneau, D.; Strain, M.J.; Sorel, M.; O'Brien, J.L.; Thompson, M.G. Qubit entanglement between ring-resonator photon-pair sources on a silicon chip. *Nat. Commun.* **2015**, *6*, 7948. https://doi.org/10.1038/ncomms8948.
87. Paesani, S.; Gentile, A.A.; Santagati, R.; Wang, J.; Wiebe, N.; Tew, D.P.; O'Brien, J.L.; Thompson, M.G. Experimental Bayesian Quantum Phase Estimation on a Silicon Photonic Chip. *Phys. Rev. Lett.* **2017**, *118*, 100503. https://doi.org/10.1103/PhysRevLett.118.100503.
88. Zeng, H.Z.J.; Ngyuen, M.A.P.; Ai, X.; Bennet, A.; Solnstev, A.S.; Laucht, A.; Al-Juboori, A.; Toth, M.; Mildren, R.P.; Malaney, R.; et al. Integrated room temperature single-photon source for quantum key distribution. *Opt. Lett.* **2022**, *47*, 1673–1676. https://doi.org/10.1364/OL.454450.
89. Beutel, F.; Gehring, H.; Wolff, M.A.; Schuck, C.; Pernice, W. Detector-integrated on-chip QKD receiver for GHz clock rates. *NPJ Quantum Inf.* **2021**, *7*, 40. https://doi.org/10.1038/s41534-021-00373-7.

90. Zheng, X.D.; Zhang, P.Y.; Ge, R.Y.; Lu, L.L.; He, G.L.; Chen, Q.; Qu, F.C.; Zhang, L.B.; Cai, X.L.; Lu, Y.Q.; et al. Heterogeneously integrated, superconducting silicon-photonic platform for measurement-device-independent quantum key distribution. *Adv. Photonics* **2021**, *3*, 055002. https://doi.org/10.1117/1.Ap.3.5.055002.
91. Sasaki, M.; Fujiwara, M.; Ishizuka, H.; Klaus, W.; Wakui, K.; Takeoka, M.; Miki, S.; Yamashita, T.; Wang, Z.; Tanaka, A.; et al. Field test of quantum key distribution in the Tokyo QKD Network. *Opt. Express* **2011**, *19*, 10387–10409. https://doi.org/10.1364/OE.19.010387.
92. Tanaka, A.; Fujiwara, M.; Yoshino, K.I.; Takahashi, S.; Nambu, Y.; Tomita, A.; Miki, S.; Yamashita, T.; Wang, Z.; Sasaki, M.; et al. High-Speed Quantum Key Distribution System for 1-Mbps Real-Time Key Generation. *IEEE J. Quantum Electron.* **2012**, *48*, 542–550. https://doi.org/10.1109/jqe.2012.2187327.
93. Ma, C.; Sacher, W.D.; Tang, Z.; Mikkelsen, J.C.; Yang, Y.; Xu, F.; Thiessen, T.; Lo, H.K.; Poon, J.K.S. Silicon photonic transmitter for polarization-encoded quantum key distribution. *Optica* **2016**, *3*, 1274–1278. https://doi.org/10.1364/OPTICA.3.001274.
94. Sibson, P.; Kennard, J.E.; Stanisic, S.; Erven, C.; O'Brien, J.L.; Thompson, M.G. Integrated silicon photonics for high-speed quantum key distribution. *Optica* **2017**, *4*, 172–177. https://doi.org/10.1364/optica.4.000172.
95. Sibson, P.; Erven, C.; Godfrey, M.; Miki, S.; Yamashita, T.; Fujiwara, M.; Sasaki, M.; Terai, H.; Tanner, M.G.; Natarajan, C.M.; et al. Chip-based quantum key distribution. *Nat. Commun.* **2017**, *8*, 13984. https://doi.org/10.1038/ncomms13984.
96. Bunandar, D.; Lentine, A.; Lee, C.; Cai, H.; Long, C.M.; Boynton, N.; Martinez, N.; DeRose, C.; Chen, C.; Grein, M.; et al. Metropolitan Quantum Key Distribution with Silicon Photonics. *Phys. Rev. X* **2018**, *8*, 021009. https://doi.org/10.1103/PhysRevX.8.021009.
97. Geng, W.; Zhang, C.; Zheng, Y.; He, J.; Zhou, C.; Kong, Y. Stable quantum key distribution using a silicon photonic transceiver. *Opt. Express* **2019**, *27*, 29045–29054. https://doi.org/10.1364/OE.27.029045.
98. Paraïso, T.K.; De Marco, I.; Roger, T.; Marangon, D.G.; Dynes, J.F.; Lucamarini, M.; Yuan, Z.; Shields, A.J. A modulator-free quantum key distribution transmitter chip. *NPJ Quantum Inf.* **2019**, *5*, 42. https://doi.org/10.1038/s41534-019-0158-7.
99. Kong, L.; Li, Z.; Li, C.; Cao, L.; Xing, Z.; Cao, J.; Wang, Y.; Cai, X.; Zhou, X. Photonic integrated quantum key distribution receiver for multiple users. *Opt. Express* **2020**, *28*, 18449–18455. https://doi.org/10.1364/OE.394050.
100. Avesani, M.; Calderaro, L.; Schiavon, M.; Stanco, A.; Agnesi, C.; Santamato, A.; Zahidy, M.; Scriminich, A.; Foletto, G.; Contestabile, G.; et al. Full daylight quantum-key-distribution at 1550 nm enabled by integrated silicon photonics. *NPJ Quantum Inf.* **2021**, *7*, 93. https://doi.org/10.1038/s41534-021-00421-2.
101. De Marco, I.; Woodward, R.I.; Roberts, G.L.; Paraïso, T.K.; Roger, T.; Sanzaro, M.; Lucamarini, M.; Yuan, Z.; Shields, A.J. Real-time operation of a multi-rate, multi-protocol quantum key distribution transmitter. *Optica* **2021**, *8*, 911–915. https://doi.org/10.1364/optica.423517.
102. Paraïso, T.K.; Roger, T.; Marangon, D.G.; De Marco, I.; Sanzaro, M.; Woodward, R.I.; Dynes, J.F.; Yuan, Z.; Shields, A.J. A photonic integrated quantum secure communication system. *Nat. Photonics* **2021**, *15*, 850–856. https://doi.org/10.1038/s41566-021-00873-0.
103. Zhang, G.; Zhao, Z.; Dai, J.; Yang, S.; Fu, X.; Yang, L. Polarization-based Quantum Key Distribution Encoder and Decoder on Silicon Photonics. *J. Light. Technol.* **2021**, *40*, 2052–2059. https://doi.org/10.1109/jlt.2021.3131193.
104. Zhu, C.X.; Chen, Z.Y.; Li, Y.; Wang, X.Z.; Wang, C.Z.; Zhu, Y.L.; Liang, F.T.; Cai, W.Q.; Jin, G.; Liao, S.K.; et al. Experimental Quantum Key Distribution with Integrated Silicon Photonics and Electronics. *Phys. Rev. Appl.* **2022**, *17*, 064034. https://doi.org/10.1103/PhysRevApplied.17.064034.
105. Zhang, G.; Chen, W.; Fan-yuan, g.j.; Zhang, L.; Wang, F.; Wang, S.; Yin, Z.Q.; He, D.; Liu, W.; An, J.; et al. Polarization-insensitive quantum key distribution using planar lightwave circuit chips. *Sci. China Inf. Sci.* **2022**, *65*, 200506. https://doi.org/10.1007/s11432-022-3514-3.
106. Honjo, T.; Inoue, K.; Takahashi, H. Differential-phase-shift quantum key distribution experiment with a planar light-wave circuit Mach–Zehnder interferometer. *Opt. Lett.* **2004**, *29*, 2797–2799. https://doi.org/10.1364/OL.29.002797.
107. Honjo, T.; Yamamoto, S.; Yamamoto, T.; Kamada, H.; Nishida, Y.; Tadanaga, O.; Asobe, M.; Inoue, K. Field trial of differential-phase-shift quantum key distribution using polarization independent frequency up-conversion detectors. *Opt. Express* **2007**, *15*, 15920–15927. https://doi.org/10.1364/OE.15.015920.
108. Cao, L.; Luo, W.; Wang, Y.X.; Zou, J.; Yan, R.D.; Cai, H.; Zhang, Y.; Hu, X.L.; Jiang, C.; Fan, W.J.; et al. Chip-Based Measurement-Device-Independent Quantum Key Distribution Using Integrated Silicon Photonic Systems. *Phys. Rev. Appl.* **2020**, *14*, 011001. https://doi.org/10.1103/PhysRevApplied.14.011001.
109. Semenenko, H.; Sibson, P.; Hart, A.; Thompson, M.G.; Rarity, J.G.; Erven, C. Chip-based measurement-device-independent quantum key distribution. *Optica* **2020**, *7*, 238–242. https://doi.org/10.1364/OPTICA.379679.
110. Wei, K.; Li, W.; Tan, H.; Li, Y.; Min, H.; Zhang, W.J.; Li, H.; You, L.; Wang, Z.; Jiang, X.; et al. High-Speed Measurement-Device-Independent Quantum Key Distribution with Integrated Silicon Photonics. *Phys. Rev. X* **2020**, *10*, 031030. https://doi.org/10.1103/PhysRevX.10.031030.
111. Li, W.; Zapatero, V.; Tan, H.; Wei, K.; Min, H.; Liu, W.Y.; Jiang, X.; Liao, S.K.; Peng, C.Z.; Curty, M.; et al. Experimental Quantum Key Distribution Secure Against Malicious Devices. *Phys. Rev. Appl.* **2021**, *15*, 034081. https://doi.org/10.1103/PhysRevApplied.15.034081.
112. Ding, Y.; Bacco, D.; Dalgaard, K.; Cai, X.; Zhou, X.; Rottwitt, K.; Oxenløwe, L.K. High-dimensional quantum key distribution based on multicore fiber using silicon photonic integrated circuits. *NPJ Quantum Inf.* **2017**, *3*, 25. https://doi.org/10.1038/s41534-017-0026-2.

113. Zhang, G.; Haw, J.Y.; Cai, H.; Xu, F.; Assad, S.M.; Fitzsimons, J.F.; Zhou, X.; Zhang, Y.; Yu, S.; Wu, J.; et al. An integrated silicon photonic chip platform for continuous-variable quantum key distribution. *Nat. Photonics* **2019**, *13*, 839–842. https://doi.org/10.1038/s41566-019-0504-5.
114. Li, L.; Huang, P.; Wang, T.; Zeng, G. Practical security of a chip-based continuous-variable quantum-key-distribution system. *Phys. Rev. A* **2021**, *103*, 032611. https://doi.org/10.1103/PhysRevA.103.032611.
115. Tan, H.; Li, W.; Zhang, L.; Wei, K.; Xu, F. Chip-Based Quantum Key Distribution against Trojan-Horse Attack. *Phys. Rev. Appl.* **2021**, *15*, 064038. https://doi.org/10.1103/PhysRevApplied.15.064038.
116. Huang, C.; Chen, Y.; Jin, L.; Geng, M.; Wang, J.; Zhang, Z.; Wei, K. Experimental secure quantum key distribution in the presence of polarization-dependent loss. *Phys. Rev. A* **2022**, *105*, 012421. https://doi.org/10.1103/PhysRevA.105.012421.
117. Orieux, A.; Diamanti, E. Recent advances on integrated quantum communications. *J. Opt.* **2016**, *18*, 083002. https://doi.org/Artn 08300210.1088/2040-8978/18/8/083002.
118. Zhang, Q.Y.; Xu, P.; Zhu, S.N. Quantum photonic network on chip. *Chin. Phys. B* **2018**, *27*, 054207. https://doi.org/Artn 05420710.1088/1674-1056/27/5/054207.
119. Slussarenko, S.; Pryde, G.J. Photonic quantum information processing: A concise review. *Appl. Phys. Rev.* **2019**, *6*, 041303. https://doi.org/10.1063/1.5115814.
120. Elshaari, A.W.; Pernice, W.; Srinivasan, K.; Benson, O.; Zwiller, V. Hybrid integrated quantum photonic circuits. *Nat. Photonics* **2020**, *14*, 285–298. https://doi.org/10.1038/s41566-020-0609-x.
121. Chen, X.; Fu, Z.; Gong, Q.; Wang, J. Quantum entanglement on photonic chips: A review. *Adv. Photonics* **2021**, *3*, 064002. https://doi.org/10.1117/1.Ap.3.6.064002.
122. Corrielli, G.; Crespi, A.; Osellame, R. Femtosecond laser micromachining for integrated quantum photonics. *Nanophotonics* **2021**, *10*, 3789–3812. https://doi.org/10.1515/nanoph-2021-0419.
123. Hao, Y.; Xiang, S.; Han, G.; Zhang, J.; Ma, X.; Zhu, Z.; Guo, X.; Zhang, Y.; Han, Y.; Song, Z.; et al. Recent progress of integrated circuits and optoelectronic chips. *Sci. China Inf. Sci.* **2021**, *64*, 201401. https://doi.org/10.1007/s11432-021-3235-7.
124. Lu, L.; Zheng, X.; Lu, Y.; Zhu, S.; Ma, X. Advances in Chip-Scale Quantum Photonic Technologies. *Adv. Quantum Technol.* **2021**, *4*, 2100068. https://doi.org/10.1002/qute.202100068.
125. Paraïso, T.K.; Woodward, R.I.; Marangon, D.G.; Lovic, V.; Yuan, Z.; Shields, A.J. Advanced Laser Technology for Quantum Communications (Tutorial Review). *Adv. Quantum Technol.* **2021**, *4*, 2100062. https://doi.org/10.1002/qute.202100062.
126. Pelucchi, E.; Fagas, G.; Aharonovich, I.; Englund, D.; Figueroa, E.; Gong, Q.; Hannes, H.; Liu, J.; Lu, C.Y.; Matsuda, N.; et al. The potential and global outlook of integrated photonics for quantum technologies. *Nat. Rev. Phys.* **2021**, *4*, 194–208. https://doi.org/10.1038/s42254-021-00398-z.
127. Wang, Q.; Zheng, Y.; Zhai, C.; Li, X.; Gong, Q.; Wang, J. Chip-based quantum communications. *J. Semicond.* **2021**, *42*, 091901. https://doi.org/10.1088/1674-4926/42/9/091901.
128. Wang, Y.; Jöns, K.D.; Sun, Z. Integrated photon-pair sources with nonlinear optics. *Appl. Phys. Rev.* **2021**, *8*, 011314. https://doi.org/10.1063/5.0030258.
129. Moody, G.; Sorger, V.J.; Blumenthal, D.J.; Juodawlkis, P.W.; Loh, W.; Sorace-Agaskar, C.; Jones, A.E.; Balram, K.C.; Matthews, J.C.F.; Laing, A.; et al. 2022 Roadmap on integrated quantum photonics. *J. Phys. Photonics* **2022**, *4*, 012501. https://doi.org/10.1088/2515-7647/ac1ef4.
130. Vajner, D.A.; Rickert, L.; Gao, T.; Kaymazlar, K.; Heindel, T. Quantum Communication Using Semiconductor Quantum Dots. *Adv. Quantum Technol.* **2022**, *5*, 2100116. https://doi.org/10.1002/qute.202100116.
131. Thew, R.; Acin, A.; Zbinden, H.; Gisin, N. Experimental realization of entangled qutrits for quantum communication. *Quantum Inf. Comput.* **2004**, *4*, 93–101. https://doi.org/10.26421/qic4.2-1.
132. Richart, D.; Fischer, Y.; Weinfurter, H. Experimental implementation of higher dimensional time–energy entanglement. *Appl. Phys. B* **2012**, *106*, 543–550. https://doi.org/10.1007/s00340-011-4854-z.
133. Kues, M.; Reimer, C.; Roztocki, P.; Cortes, L.R.; Sciara, S.; Wetzel, B.; Zhang, Y.; Cino, A.; Chu, S.T.; Little, B.E.; et al. On-chip generation of high-dimensional entangled quantum states and their coherent control. *Nature* **2017**, *546*, 622–626. https://doi.org/10.1038/nature22986.
134. Imany, P.; Jaramillo-Villegas, J.A.; Odele, O.D.; Han, K.; Leaird, D.E.; Lukens, J.M.; Lougovski, P.; Qi, M.; Weiner, A.M. 50-GHz-spaced comb of high-dimensional frequency-bin entangled photons from an on-chip silicon nitride microresonator. *Opt. Express* **2018**, *26*, 1825–1840. https://doi.org/10.1364/OE.26.001825.
135. Schaeff, C.; Polster, R.; Huber, M.; Ramelow, S.; Zeilinger, A. Experimental access to higher-dimensional entangled quantum systems using integrated optics. *Optica* **2015**, *2*, 523–529. https://doi.org/10.1364/optica.2.000523.
136. Dada, A.C.; Leach, J.; Buller, G.S.; Padgett, M.J.; Andersson, E. Experimental high-dimensional two-photon entanglement and violations of generalized Bell inequalities. *Nat. Phys.* **2011**, *7*, 677–680. https://doi.org/10.1038/nphys1996.
137. Wang, X.L.; Cai, X.D.; Su, Z.E.; Chen, M.C.; Wu, D.; Li, L.; Liu, N.L.; Lu, C.Y.; Pan, J.W. Quantum teleportation of multiple degrees of freedom of a single photon. *Nature* **2015**, *518*, 516–519. https://doi.org/10.1038/nature14246.
138. Reimer, C.; Sciara, S.; Roztocki, P.; Islam, M.; Cortes, L.R.; Zhang, Y.B.; Fischer, B.; Loranger, S.; Kashyap, R.; Cino, A.; et al. High-dimensional one-way quantum processing implemented on d-level cluster states. *Nat. Phys.* **2019**, *15*, 148–153. https://doi.org/10.1038/s41567-018-0347-x.

139. Matthews, J.C.F.; Politi, A.; Stefanov, A.; O'Brien, J.L. Manipulation of multiphoton entanglement in waveguide quantum circuits. *Nat. Photonics* **2009**, *3*, 346–350. https://doi.org/10.1038/nphoton.2009.93.
140. Laing, A.; Peruzzo, A.; Politi, A.; Verde, M.R.; Halder, M.; Ralph, T.C.; Thompson, M.G.; O'Brien, J.L. High-fidelity operation of quantum photonic circuits. *Appl. Phys. Lett.* **2010**, *97*, 211109. https://doi.org/10.1063/1.3497087.
141. Shadbolt, P.J.; Verde, M.R.; Peruzzo, A.; Politi, A.; Laing, A.; Lobino, M.; Matthews, J.C.F.; Thompson, M.G.; O'Brien, J.L. Generating, manipulating and measuring entanglement and mixture with a reconfigurable photonic circuit. *Nat. Photonics* **2012**, *6*, 45–49. https://doi.org/10.1038/nphoton.2011.283.
142. Takesue, H.; Tokura, Y.; Fukuda, H.; Tsuchizawa, T.; Watanabe, T.; Yamada, K.; Itabashi, S.i. Entanglement generation using silicon wire waveguide. *Appl. Phys. Lett.* **2007**, *91*, 201108. https://doi.org/10.1063/1.2814040.
143. Pernice, W.H.; Schuck, C.; Minaeva, O.; Li, M.; Goltsman, G.N.; Sergienko, A.V.; Tang, H.X. High-speed and high-efficiency travelling wave single-photon detectors embedded in nanophotonic circuits. *Nat. Commun.* **2012**, *3*, 1325. https://doi.org/10.1038/ncomms2307.
144. Bonneau, D.; Engin, E.; Ohira, K.; Suzuki, N.; Yoshida, H.; Iizuka, N.; Ezaki, M.; Natarajan, C.M.; Tanner, M.G.; Hadfield, R.H.; et al. Quantum interference and manipulation of entanglement in silicon wire waveguide quantum circuits. *New J. Phys.* **2012**, *14*, 045003. https://doi.org/10.1088/1367-2630/14/4/045003.
145. Silverstone, J.W.; Bonneau, D.; Ohira, K.; Suzuki, N.; Yoshida, H.; Iizuka, N.; Ezaki, M.; Natarajan, C.M.; Tanner, M.G.; Hadfield, R.H.; et al. On-chip quantum interference between silicon photon-pair sources. *Nat. Photonics* **2013**, *8*, 104–108. https://doi.org/10.1038/nphoton.2013.339.
146. Zhang, M.; Feng, L.T.; Zhou, Z.Y.; Chen, Y.; Wu, H.; Li, M.; Gao, S.M.; Guo, G.P.; Guo, G.C.; Dai, D.X.; et al. Generation of multiphoton quantum states on silicon. *Light Sci. Appl.* **2019**, *8*, 41. https://doi.org/10.1038/s41377-019-0153-y.
147. Dutt, A.; Luke, K.; Manipatruni, S.; Gaeta, A.L.; Nussenzveig, P.; Lipson, M. On-Chip Optical Squeezing. *Phys. Rev. Appl.* **2015**, *3*, 044005. https://doi.org/10.1103/PhysRevApplied.3.044005.
148. Schuck, C.; Guo, X.; Fan, L.; Ma, X.; Poot, M.; Tang, H.X. Quantum interference in heterogeneous superconducting-photonic circuits on a silicon chip. *Nat. Commun.* **2016**, *7*, 10352. https://doi.org/10.1038/ncomms10352.
149. Zhang, X.; Bell, B.A.; Mahendra, A.; Xiong, C.; Leong, P.H.W.; Eggleton, B.J. Integrated silicon nitride time-bin entanglement circuits. *Opt. Lett.* **2018**, *43*, 3469–3472. https://doi.org/10.1364/OL.43.003469.
150. Lu, X.; Li, Q.; Westly, D.A.; Moille, G.; Singh, A.; Anant, V.; Srinivasan, K. Chip-integrated visible-telecom photon pair sources for quantum communication. *Nat. Phys.* **2019**, *15*, 373–381. https://doi.org/10.1038/s41567-018-0394-3.
151. Guidry, M.A.; Yang, K.Y.; Lukin, D.M.; Markosyan, A.; Yang, J.; Fejer, M.M.; Vučković, J. Optical parametric oscillation in silicon carbide nanophotonics. *Optica* **2020**, *7*, 1139–1142. https://doi.org/10.1364/optica.394138.
152. Tanzilli, S.; Tittel, W.; De Riedmatten, H.; Zbinden, H.; Baldi, P.; De Micheli, M.; Ostrowsky, D.B.; Gisin, N. PPLN waveguide for quantum communication. *Eur. Phys. J. D* **2002**, *18*, 155–160. https://doi.org/10.1140/epjd/e20020019.
153. Jin, H.; Liu, F.M.; Xu, P.; Xia, J.L.; Zhong, M.L.; Yuan, Y.; Zhou, J.W.; Gong, Y.X.; Wang, W.; Zhu, S.N. On-chip generation and manipulation of entangled photons based on reconfigurable lithium-niobate waveguide circuits. *Phys. Rev. Lett.* **2014**, *113*, 103601. https://doi.org/10.1103/PhysRevLett.113.103601.
154. Höpker, J.P.; Bartnick, M.; Meyer-Scott, E.; Thiele, F.; Krapick, S.; Montaut, N.; Santandrea, M.; Herrmann, H.; Lengeling, S.; Ricken, R. Towards integrated superconducting detectors on lithium niobate waveguides. In *Quantum Photonic Devices*; SPIE: Bellingham, WA, USA, 2017; Volume 10358, pp. 21–27. https://doi.org/10.1117/12.2273388.
155. Sprengers, J.P.; Gaggero, A.; Sahin, D.; Jahanmirinejad, S.; Frucci, G.; Mattioli, F.; Leoni, R.; Beetz, J.; Lermer, M.; Kamp, M.; et al. Waveguide superconducting single-photon detectors for integrated quantum photonic circuits. *Appl. Phys. Lett.* **2011**, *99*, 181110. https://doi.org/10.1063/1.3657518.
156. Horn, R.; Abolghasem, P.; Bijlani, B.J.; Kang, D.; Helmy, A.S.; Weihs, G. Monolithic source of photon pairs. *Phys. Rev. Lett.* **2012**, *108*, 153605. https://doi.org/10.1103/PhysRevLett.108.153605.
157. Wang, J.; Santamato, A.; Jiang, P.; Bonneau, D.; Engin, E.; Silverstone, J.W.; Lermer, M.; Beetz, J.; Kamp, M.; Höfling, S.; et al. Gallium arsenide (GaAs) quantum photonic waveguide circuits. *Opt. Commun.* **2014**, *327*, 49–55. https://doi.org/10.1016/j.optcom.2014.02.040.
158. Abellan, C.; Amaya, W.; Domenech, D.; Muñoz, P.; Capmany, J.; Longhi, S.; Mitchell, M.W.; Pruneri, V. Quantum entropy source on an InP photonic integrated circuit for random number generation. *Optica* **2016**, *3*, 989–994. https://doi.org/10.1364/optica.3.000989.
159. Sipahigil, A.; Evans, R.E.; Sukachev, D.D.; Burek, M.J.; Borregaard, J.; Bhaskar, M.K.; Nguyen, C.T.; Pacheco, J.L.; Atikian, H.A.; Meuwly, C.; et al. An integrated diamond nanophotonics platform for quantum-optical networks. *Science* **2016**, *354*, 847–850. https://doi.org/10.1126/science.aah6875.
160. Meany, T.; Gräfe, M.; Heilmann, R.; Perez-Leija, A.; Gross, S.; Steel, M.J.; Withford, M.J.; Szameit, A. Laser written circuits for quantum photonics. *Laser Photonics Rev.* **2015**, *9*, 363–384. https://doi.org/10.1002/lpor.201500061.
161. Boada, O.; Novo, L.; Sciarrino, F.; Omar, Y. Quantum walks in synthetic gauge fields with three-dimensional integrated photonics. *Phys. Rev. A* **2017**, *95*, 013830. https://doi.org/10.1103/PhysRevA.95.013830.
162. Tang, H.; Lin, X.F.; Feng, Z.; Chen, J.Y.; Gao, J.; Sun, K.; Wang, C.Y.; Lai, P.C.; Xu, X.Y.; Wang, Y.; et al. Experimental two-dimensional quantum walk on a photonic chip. *Sci. Adv.* **2018**, *4*, eaat3174. https://doi.org/10.1126/sciadv.aat3174.

163. Zeuner, J.; Pitsios, I.; Tan, S.H.; Sharma, A.N.; Fitzsimons, J.F.; Osellame, R.; Walther, P. Experimental quantum homomorphic encryption. *NPJ Quantum Inf.* **2021**, *7*, 25. https://doi.org/10.1038/s41534-020-00340-8.
164. Wang, J.; Bonneau, D.; Villa, M.; Silverstone, J.W.; Santagati, R.; Miki, S.; Yamashita, T.; Fujiwara, M.; Sasaki, M.; Terai, H.; et al. Chip-to-chip quantum photonic interconnect by path-polarization interconversion. *Optica* **2016**, *3*, 407–413. https://doi.org/10.1364/optica.3.000407.
165. Kwek, L.C.; Cao, L.; Luo, W.; Wang, Y.; Sun, S.; Wang, X.; Liu, A.Q. Chip-based quantum key distribution. *AAPPS Bull.* **2021**, *31*, 15. https://doi.org/10.1007/s43673-021-00017-0.
166. Wang, C.; Zhang, M.; Chen, X.; Bertrand, M.; Shams-Ansari, A.; Chandrasekhar, S.; Winzer, P.; Loncar, M. Integrated lithium niobate electro-optic modulators operating at CMOS-compatible voltages. *Nature* **2018**, *562*, 101–104. https://doi.org/10.1038/s41586-018-0551-y.
167. He, M.; Xu, M.; Ren, Y.; Jian, J.; Ruan, Z.; Xu, Y.; Gao, S.; Sun, S.; Wen, X.; Zhou, L.; et al. High-performance hybrid silicon and lithium niobate Mach-Zehnder modulators for 100 Gbits s-1 and beyond. *Nat. Photonics* **2019**, *13*, 359–364. https://doi.org/10.1038/s41566-019-0378-6.
168. Zhang, J.; Itzler, M.A.; Zbinden, H.; Pan, J.W. Advances in InGaAs/InP single-photon detector systems for quantum communication. *Light-Sci. Appl.* **2015**, *4*, e286. https://doi.org/10.1038/lsa.2015.59.
169. Comandar, L.C.; Fröhlich, B.; Dynes, J.F.; Sharpe, A.W.; Lucamarini, M.; Yuan, Z.L.; Penty, R.V.; Shields, A.J. Gigahertz-gated InGaAs/InP single-photon detector with detection efficiency exceeding 55% at 1550 nm. *J. Appl. Phys.* **2015**, *117*, 083109. https://doi.org/10.1063/1.4913527.
170. Amri, E.; Boso, G.; Korzh, B.; Zbinden, H. Temporal jitter in free-running InGaAs/InP single-photon avalanche detectors. *Opt. Lett.* **2016**, *41*, 5728–5731. https://doi.org/10.1364/OL.41.005728.
171. Hadfield, R.H. Single-photon detectors for optical quantum information applications. *Nat. Photonics* **2009**, *3*, 696–705. https://doi.org/10.1038/nphoton.2009.230.
172. Natarajan, C.M.; Tanner, M.G.; Hadfield, R.H. Superconducting nanowire single-photon detectors: Physics and applications. *Supercond. Sci. Technol.* **2012**, *25*, 063001. https://doi.org/10.1088/0953-2048/25/6/063001.
173. You, L. Superconducting nanowire single-photon detectors for quantum information. *Nanophotonics* **2020**, *9*, 2673–2692. https://doi.org/doi:10.1515/nanoph-2020-0186.
174. Caloz, M.; Perrenoud, M.; Autebert, C.; Korzh, B.; Weiss, M.; Schönenberger, C.; Warburton, R.J.; Zbinden, H.; Bussières, F. High-detection efficiency and low-timing jitter with amorphous superconducting nanowire single-photon detectors. *Appl. Phys. Lett.* **2018**, *112*, 061103. https://doi.org/10.1063/1.5010102.
175. Ferrari, S.; Schuck, C.; Pernice, W. Waveguide-integrated superconducting nanowire single-photon detectors. *Nanophotonics* **2018**, *7*, 1725–1758.
176. Tang, G.; Li, C.; Wang, M. Polarization discriminated time-bin phase-encoding measurement-device-independent quantum key distribution. *Quant. Eng.* **2021**, *3*, e79. https://doi.org/10.1002/que2.79.
177. Guo, H.; Li, Z.; Yu, S.; Zhang, Y. Toward practical quantum key distribution using telecom components. *Fundam. Res.* **2021**, *1*, 96–98. https://doi.org/10.1016/j.fmre.2020.12.002.
178. Grosshans, F.; Grangier, P. Continuous variable quantum cryptography using coherent states. *Phys. Rev. Lett.* **2002**, *88*, 057902. https://doi.org/10.1103/PhysRevLett.88.057902.
179. Weedbrook, C.; Lance, A.M.; Bowen, W.P.; Symul, T.; Ralph, T.C.; Lam, P.K. Quantum cryptography without switching. *Phys. Rev. Lett.* **2004**, *93*, 170504. https://doi.org/10.1103/PhysRevLett.93.170504.
180. Cerf, N.J.; Lévy, M.; Assche, G.V. Quantum distribution of Gaussian keys using squeezed states. *Phys. Rev. A* **2001**, *63*, 052311. https://doi.org/10.1103/PhysRevA.63.052311.
181. Ralph, T.C. Continuous variable quantum cryptography. *Phys. Rev. A* **1999**, *61*, 010303. https://doi.org/10.1103/PhysRevA.61.010303.
182. Gisin, N.; Fasel, S.; Kraus, B.; Zbinden, H.; Ribordy, G. Trojan-horse attacks on quantum-key-distribution systems. *Phys. Rev. A* **2006**, *73*, 022320. https://doi.org/10.1103/PhysRevA.73.022320.
183. Li, H.W.; Wang, S.; Huang, J.Z.; Chen, W.; Yin, Z.Q.; Li, F.Y.; Zhou, Z.; Liu, D.; Zhang, Y.; Guo, G.C.; et al. Attacking a practical quantum-key-distribution system with wavelength-dependent beam-splitter and multiwavelength sources. *Phys. Rev. A* **2011**, *84*, 062308. https://doi.org/10.1103/PhysRevA.84.062308.
184. Sajeed, S.; Radchenko, I.; Kaiser, S.; Bourgoin, J.P.; Pappa, A.; Monat, L.; Legré, M.; Makarov, V. Attacks exploiting deviation of mean photon number in quantum key distribution and coin tossing. *Phys. Rev. A* **2015**, *91*, 032326.
185. Qi, B.; Fred, F.C.h.; Lo, H.K.; Ma, X. Time-shift attack in practical quantum cryptosystems. *Quant. Inf. Comput.* **2007**, *7*, 73–82.
186. Yoshino, K.i.; Fujiwara, M.; Nakata, K.; Sumiya, T.; Sasaki, T.; Takeoka, M.; Sasaki, M.; Tajima, A.; Koashi, M.; Tomita, A. Quantum key distribution with an efficient countermeasure against correlated intensity fluctuations in optical pulses. *Npj Quantum Inf.* **2018**, *4*, 8. https://doi.org/10.1038/s41534-017-0057-8.
187. Lydersen, L.; Wiechers, C.; Wittmann, C.; Elser, D.; Skaar, J.; Makarov, V. Hacking commercial quantum cryptography systems by tailored bright illumination. *Nat. Photonics* **2010**, *4*, 686–689. https://doi.org/10.1038/nphoton.2010.214.
188. Henning, W.; Harald, K.; Markus, R.; Martin, F.; Sebastian, N.; Harald, W. Quantum eavesdropping without interception: An attack exploiting the dead time of single-photon detectors. *New J. Phys.* **2011**, *13*, 073024.

189. Wei, K.; Liu, H.; Ma, H.; Yang, X.; Zhang, Y.; Sun, Y.; Xiao, J.; Ji, Y. Feasible attack on detector-device-independent quantum key distribution. *Sci. Rep.* **2017**, *7*, 449. https://doi.org/10.1038/s41598-017-00531-y.
190. Wei, K.; Zhang, W.; Tang, Y.L.; You, L.; Xu, F. Implementation security of quantum key distribution due to polarization-dependent efficiency mismatch. *Phys. Rev. A* **2019**, *100*, 022325. https://doi.org/10.1103/PhysRevA.100.022325.
191. Xu, F.; Wei, K.; Sajeed, S.; Kaiser, S.; Sun, S.; Tang, Z.; Qian, L.; Makarov, V.; Lo, H.K. Experimental quantum key distribution with source flaws. *Phys. Rev. A* **2015**, *92*, 032305.
192. Tang, Z.; Wei, K.; Bedroya, O.; Qian, L.; Lo, H.K. Experimental measurement-device-independent quantum key distribution with imperfect sources. *Phys. Rev. A* **2016**, *93*, 042308.
193. Tamaki, K.; Curty, M.; Lucamarini, M. Decoy-state quantum key distribution with a leaky source. *New J. Phys.* **2016**, *18*, 065008. https://doi.org/10.1088/1367-2630/18/6/065008.
194. Lucamarini, M.; Choi, I.; Ward, M.; Dynes, J.; Yuan, Z.; Shields, A. Practical Security Bounds Against the Trojan-Horse Attack in Quantum Key Distribution. *Phys. Rev. X* **2015**, *5*, 031030.
195. Pereira, M.; Kato, G.; Mizutani, A.; Curty, M.; Tamaki, K. Quantum key distribution with correlated sources. *Sci. Adv.* **2020**, *6*, eaaz4487. https://doi.org/doi:10.1126/sciadv.aaz4487.
196. Zhang, Y.; Coles, P.J.; Winick, A.; Lin, J.; Lütkenhaus, N. Security proof of practical quantum key distribution with detection-efficiency mismatch. *Phys. Rev. Res.* **2021**, *3*, 013076. https://doi.org/10.1103/PhysRevResearch.3.013076.
197. Chen, Y.; Huang, C.; Chen, Z.; He, W.; Zhang, C.; Sun, S.; Wei, K. Experimental study of secure quantum key distribution with source and detection imperfections. *Phys. Rev. A* **2022**, *106*, 022614. https://doi.org/10.1103/PhysRevA.106.022614.
198. Lo, H.K.; Curty, M.; Tamaki, K. Secure quantum key distribution. *Nat. Photonics* **2014**, *8*, 595–604. https://doi.org/10.1038/nphoton.2014.149.
199. Lucamarini, M.; Yuan, Z.L.; Dynes, J.F.; Shields, A.J. Overcoming the rate-distance limit of quantum key distribution without quantum repeaters. *Nature* **2018**, *557*, 400–403. https://doi.org/10.1038/s41586-018-0066-6.
200. Yin, Z.Q.; Lu, F.Y.; Teng, J.; Wang, S.; Chen, W.; Guo, G.C.; Han, Z.F. Twin-field protocols: Towards intercity quantum key distribution without quantum repeaters. *Fundam. Res.* **2021**, *1*, 93–95. https://doi.org/10.1016/j.fmre.2020.11.001.
201. Pirandola, S.; Laurenza, R.; Ottaviani, C.; Banchi, L. Fundamental limits of repeaterless quantum communications. *Nat. Commun.* **2017**, *8*, 15043. https://doi.org/10.1038/ncomms15043.
202. Ma, X.F.; Zeng, P.; Zhou, H.Y. Phase-Matching Quantum Key Distribution. *Phys. Rev. X* **2018**, *8*, 031043. https://doi.org/10.1103/PhysRevX.8.031043.
203. Wang, X.B.; Yu, Z.W.; Hu, X.L. Twin-field quantum key distribution with large misalignment error. *Phys. Rev. A* **2018**, *98*, 062323. https://doi.org/10.1103/PhysRevA.98.062323.
204. Wang, S.; He, D.Y.; Yin, Z.Q.; Lu, F.Y.; Cui, C.H.; Chen, W.; Zhou, Z.; Guo, G.C.; Han, Z.F. Beating the Fundamental Rate-Distance Limit in a Proof-of-Principle Quantum Key Distribution System. *Phys. Rev. X* **2019**, *9*, 021046. https://doi.org/10.1103/PhysRevX.9.021046.