Smart Materials and Devices

Science Exploration

Open Access Review

Recent advances in photonic integrated chips for quantum key distribution: Protocol requirements and system deployment

Jin You[1], Xia Yin[2], Songrui Yang[1], Chuqiao Hu[3], Pengle Cheng[1], Junming An[4,*]

[1]School of Technology, Beijing Forestry University, Beijing 100083, China.
[2]Center for High Pressure Science and Technology Advanced Research (HPSTAR), Beijing 100193, China.
[3]College of Information Science and Technology, Dalian Maritime University, Dalian 116026, Liaoning, China.
[4]State Key Laboratory of Integrated Optoelectronics, Institute of Semiconductors, Chinese Academy of Sciences, Beijing 100083, China.

***Correspondence to:** Junming An, State Key Laboratory of Integrated Optoelectronics, Institute of Semiconductors, Chinese Academy of Sciences, Beijing 100083, China. E-mail: junming@semi.ac.cn

Received: July 10, 2026 **Accepted:** October 14, 2026 **Published:** November 03, 2026

Cite this article: You J, Yin X, Yang S, Hu C, Cheng P, An J. Recent advances in photonic integrated chips for quantum key distribution: Protocol requirements and system deployment. Smart Mater Devices. 2027;3:202638. https://doi.org/10.70401/smd.2026.0062

Abstract

Quantum key distribution (QKD) is moving from laboratory demonstrations toward network deployment, and integrated photonic chips provide a hardware route for compact, stable and scalable systems. This review summarizes progress in integrated photonic chips for QKD from protocol requirements to deployable systems. It first examines how decoy-state BB84, measurement-device-independent QKD (MDI-QKD), twin-field QKD (TF-QKD), continuous-variable QKD (CV-QKD) and device-independent QKD (DI-QKD) constrain chip metrics such as loss, modulation accuracy, state indistinguishability, phase stability, synchronization and security monitoring. It then compares planar lightwave circuit (PLC), silicon photonics, silicon nitride, thin-film lithium niobate, indium phosphide (InP) and heterogeneous platforms in terms of routing loss, modulation speed, stable interference, source integration and detector interfaces. Transmitter and receiver architectures, coherent detection, single-photon detection interfaces and on-chip monitoring are discussed as system-level building blocks. The review further analyses phase stability, packaging coupling, thermal management, polarization control, network coexistence and reliability, emphasizing that deployable QKD chips must remain calibratable and compatible with security models under realistic operation. Finally, system demonstrations, network deployment and practical security are discussed within a unified evaluation framework. Throughout, we argue that integration benefits QKD only when compact routing, stable interference, calibration access and manufacturable packaging jointly keep the device inside the assumptions of its security proof; accordingly, chip performance should be judged by mapped, calibratable security parameters rather than by integration density alone.

Keywords: Quantum key distribution, photonic integrated chips, practical security, protocol requirements, system deployment

1. Introduction

Quantum key distribution (QKD) establishes secret keys from quantum no-cloning, measurement disturbance and composable-security principles, rather than from computational hardness alone. Since BB84, entanglement-based QKD, decoy-state protocols, measurement-device-independent QKD (MDI-QKD), device-independent QKD (DI-QKD), twin-field QKD (TF-QKD) and continuous-variable QKD (CV-QKD) have progressively expanded the security and implementation landscape[1-3]. This evolution has also changed the hardware problem. A practical QKD apparatus must prepare, transmit, measure and monitor quantum states while keeping the physical device inside the assumptions of the security proof[3-5].

QKD has moved beyond isolated laboratory links. Fiber links, free-space channels, satellite experiments and metropolitan networks, including the Tokyo QKD Network and the 4,600-km integrated space-to-ground quantum communication network, have shown that QKD can operate across multi-node and cross-domain communication infrastructures[6-9]. These demonstrations also clarify the engineering bottleneck. Deployable systems require low optical loss, stable encoding, compact packaging, repeatable calibration, thermal robustness, manufacturable components and interfaces compatible with classical network control.

Integrated photonic chips provide a direct route to this form of hardware consolidation. On planar lightwave circuit (PLC), silicon photonic, silicon nitride, thin-film lithium niobate, indium phosphide (InP) and hybrid platforms, interferometers, couplers, beam splitters, phase and intensity modulators, attenuators, filters, monitoring paths and detector interfaces can be integrated within

© The Author(s) 2026. This is an Open Access article licensed under a Creative Commons Attribution 4.0 International License (https://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, sharing, adaptation, distribution and reproduction in any medium or format, for any purpose, even commercially, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made.

compact optical modules[10-13]. The framework in Figure 1 organizes this transition from protocol demand to chip response: shortened optical paths and monolithic alignment primarily improve stability, whereas wafer-scale fabrication and on-chip monitoring turn security-relevant quantities into measurable engineering parameters. These parameters include loss, extinction ratio, phase error, polarization-dependent loss, crosstalk, timing jitter and calibration stability.

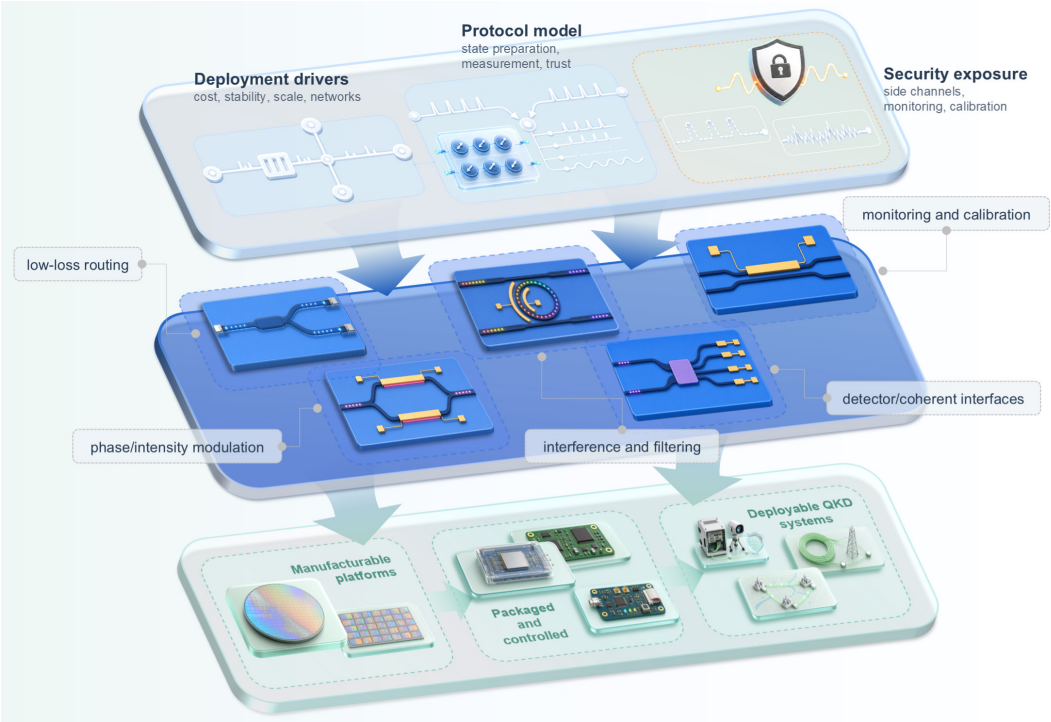


Figure 1. Protocol-to-hardware framework for integrated photonic QKD chips. The diagram links deployment requirements, protocol assumptions and chip-level responses, emphasizing that integration is valuable only when compact routing, stable interference, calibration access and manufacturable packaging jointly preserve the security model. QKD: quantum key distribution.

Chip-based QKD has evolved from PLC interferometric modules toward diverse photonic platforms. Early silica and silicon PLC studies integrated BB84, differential-phase-shift QKD and polarization-insensitive receiver functions, demonstrating the stability advantages of planar interferometers[14-16]. Silicon-photonic QKD transmitters and transceivers later compressed phase, intensity and polarization encoding into compact chips, while integrated continuous-variable QKD (CV-QKD) and heterogeneous photonics extended the design space toward coherent receivers, electro-optic modulation and source-detector interfaces[13,17,18].

Different QKD protocols impose different chip requirements. Decoy-state BB84 requires high-extinction intensity modulation, phase randomization and limited state-dependent leakage[19-21]. MDI-QKD requires high-indistinguishability interference between independent users[22,23], whereas TF-QKD is dominated by remote phase reference, frequency locking and long-term stability. CV-QKD relies on linear modulation, low-noise coherent detection, balanced photodetection and high-speed digital signal processing[24,25]. A chip that performs well for one protocol may therefore be unsuitable for another if its non-idealities fall outside the corresponding security model.

Integration does not automatically improve security. Detector-blinding, time-shift and local-oscillator attacks have shown that practical QKD systems can fail when device behaviour deviates from model assumptions[26-28]. Chip integration may suppress some alignment and drift problems, but it can also introduce new forms of reflection feedback, residual modulation, thermal crosstalk, electrical coupling and package-dependent leakage. The main challenge is therefore to align protocol models, chip metrics and deployable packaging within one security-aware evaluation framework.

Existing reviews have summarized QKD from the perspectives of practical security, realistic devices, CV-QKD systems, QKD networking and chip-based QKD[2-4,29]. For PLC and integrated photonic QKD chips, however, the key task is to connect protocol requirements, device metrics, platform trade-offs and deployable systems. The organizing contribution of this review is a traceable connection between these levels: protocol-specific trust assumptions identify the device quantities that must be characterized; platform and package choices determine how those quantities can be measured and controlled; and system demonstrations establish the conditions under which secure keys are obtained. Table 1 and Table 2 organize protocol and platform constraints, whereas Table 3 and Table 4 distinguish system evidence from proposed reporting requirements. The framework is intended to support comparison under stated operating and security assumptions, rather than to rank platforms by integration density alone.

Table 1. Protocol-specific chip constraints and trust boundaries. The comparison separates the dominant optical functions, measurable device metrics and security assumptions for major QKD protocol classes, providing a checklist for matching chip architecture to protocol model.

Protocol class	Main chip-level constraints	Critical security boundary	Representative contribution and evidence
Decoy-state BB84	Intensity accuracy, phase randomization, extinction ratio, state indistinguishability	Source statistics and side-channel leakage	Single-photon estimation using decoy intensities[19,20]; source-state requirements[21].
MDI-QKD	Two-photon interference, user indistinguishability, synchronization, Bell-state measurement stability	Untrusted measurement station; characterized sources and authenticated classical communication	Untrusted measurement-node security[22,23]; chip implementation[32,34].
TF-QKD/SNS-QKD	Remote phase reference, frequency locking, phase tracking and long-term coherence	Single-photon interference between distant users	Rate-distance motivation[36]; long-distance and field-link demonstrations[37,38,141].
CV-QKD	Linear modulation, shot-noise calibration, balanced detection, excess-noise estimation and DSP	Trusted receiver model and coherent-detection calibration	Coherent-state framework[24]; local oscillator[25]; composable implementation[33]; integrated reception[41].
DI-QKD	Detection efficiency, loss tolerance, Bell-test loophole closure and finite-key size	Minimal device trust based on Bell violation	Security framework[5]; device-independent protocol review[48].

MDI-QKD: measurement-device-independent QKD; TF-QKD: twin-field QKD; CV-QKD: continuous-variable QKD; DI-QKD: device-independent QKD; DSP: digital signal processing; SNS-QKD: sending-or-not-sending quantum key distribution.

Table 2. Platform trade-offs, loss definitions and evidence of process maturity. Numerical examples describe the cited devices and geometries, and the maturity column records documented fabrication or implementation evidence.

Platform	QKD function and limitation	Loss evidence and boundary	Process maturity evidence	Sources
Silica PLC	Stable passive encoding/decoding; relatively large footprint and external high-speed modulation.	Report propagation, fiber coupling and interferometer insertion loss separately; no platform-wide value assigned.	Established encoder/decoder and long-path interferometer demonstrations; packaged performance remains design-specific.	[14,15,52,53]
Silicon photonics	Dense encoding and electronic integration; carrier effects, coupling and polarization need control.	Active-device, grating/edge coupling and passive routing losses must be separated; channel attenuation is not chip loss.	CMOS-compatible fabrication and photonic-electronic QKD demonstrations; these do not by themselves establish production yield.	[12,31,57,58]
Silicon nitride	Passive delay/filter circuits; native high-speed modulation is limited.	TriPleX single-stripe example: 0.03 dB/cm at 1.55 μm and 2 mm bend radius; not packaged-module loss[61].	Documented building blocks, design kits and multi-project wafer access in the cited process overview[61].	[60,61]
Thin-film lithium niobate	High-speed Pockels modulation; RF and optical interfaces require co-design.	Reported modulator on-chip loss < 0.5 dB; distinct from propagation loss per unit length[51].	Monolithic and hybrid modulator demonstrations; reproducibility and package qualification require separate evidence.	[51,65]
InP	Monolithic active sources and modulation; gain, reflections and thermal control affect operation.	Specify active/passive transition and coupling losses for the actual circuit; no universal loss value assigned.	Generic integration technology with reusable active/passive building blocks; QKD qualification is a separate step.	[66]

Heterogeneous integration	Allocates gain, routing, modulation and detection across materials; introduces additional interfaces.	Include inter-material coupling, bonding interfaces and package connections in the end-to-end budget.	Assembly strategy, not one material or process; alignment, bonding yield and thermal compatibility are design-specific.	[49,67-69]

PLC: planar lightwave circuit; CMOS: complementary metal-oxide-semiconductor; QKD: quantum key distribution; InP: indium phosphide; RF: radio frequency.

Table 3. Individual QKD demonstrations and reference benchmarks. Each row corresponds to one study and distinguishes protocol, integrated functions, operating conditions and the meaning of the reported metric.

Study and protocol	Integrated functions and conditions	Reported result and security/comparison boundary	Ref.
Bunandar *et al*. DV-QKD	Silicon-photonic transmitter; 43 km metropolitan fiber; 16.4 dB link loss.	157 kbit/s composable secret-key rate. Tests deployed-link operation; does not establish a platform-wide rate advantage.	[12]
Avesani *et al*. DV-QKD	Silicon-photonic transmitter; 145 m daylight free-space link at 1,550 nm.	About 30 kbit/s average secret-key rate and 0.5% QBER. Daylight tracking and background conditions differ from fiber tests.	[110]
Wei *et al*. MDI-QKD	Two silicon-photonic user transmitters; 1.25 GHz clock; off-chip measurement station.	31 bit/s finite-key rate at 36 dB channel loss (180 km equivalent standard fiber); 497 bit/s reported separately over 140 km fiber spools.	[34]
Hajomer *et al* .CV-QKD	Integrated photonic-electronic receiver; 10 GBd; 5 and 10 km fiber; offline DSP.	Estimated 0.737 and 0.315 Gbit/s respectively, with finite-size parameter-estimation effects under collective attacks and assumed reconciliation efficiency; not real-time composable key delivery.	[41]
Zhu *et al*. One-decoy DV-QKD	PLC integration modules; 625 MHz; advantage distillation.	Composable rates: 3.32 Mbit/s at 2 dB and 1.85 kbit/s at 18 dB. Loss and post-processing choices are part of the comparison.	[115]
Liu *et al*. 8-PSK CV-QKD	Silicon-photonic transmitter and receiver; 1.5625 GBd; 25.8 and 50.4 km fiber.	Asymptotic rates: 31.05 and 5.05 Mbit/s respectively. These should not be ranked directly against finite-key/composable rates.	[116]
Cao *et al*. CV-QKD	Integrated CV-QKD implementation with external laser; 50 km; 12 h operation.	Reported mean rate 0.737 Mbit/s. The stability interval is distinct from a cross-platform security comparison; apply the original study's security model.	[117]
Yan *et al*. MDI network	Optical-frequency-comb network; about 30 dB link attenuation; two pairs active simultaneously.	Average 267 bit/s per user pair. Report active pairs and shared resources separately from projected network capacity.	[124]
Zheng *et al*. TF network	20 client transmitter chips; server microcomb; ten wavelength channels; 370 km spooled fiber.	Sequential pairwise tests. The 3,700 km aggregate networking metric is not one link or proof that all pairs operate simultaneously.	[125]
Li *et al*. High-rate DV benchmark	Reference high-rate system; 10 km standard fiber; not a matched-condition chip-platform test.	Secret-key rate above 110 Mbit/s. Detector, clock and processing resources must be included when comparing with integrated systems.	[120]
Boaron *et al*. Long-distance DV benchmark	421 km fiber link; reference long-distance implementation.	Demonstrates secure operation at long distance, not network span or an integration advantage. It is retained as a distance benchmark.	[121]

QKD: quantum key distribution; DV-QKD: discrete-variable QKD; QBER: quantum bit error rate; MDI-QKD: measurement-device-independent QKD; CV-QKD: continuous-variable QKD; PLC: planar lightwave circuit; DSP: digital signal processing; PSK: phase-shift keying.

Table 4. Consolidated evaluation dimensions for integrated QKD chips derived from recent security, network and platform studies.

Evaluation dimension	What recent work establishes	Requirement on chip specification	Evidence by topic
CV-QKD security	Finite-size discrete-modulation security; trusted detector noise; nonideal heterodyne detection	Specify modulation, detector trust, finite-size assumptions and calibrated parameters	Finite-size discrete modulation[46]; nonideal heterodyne[47]; trusted detector noise[101]; discrete-modulation security[142].
Calibration and source errors	Shot-noise calibration; source-intensity errors; phase-reference-intensity attacks	Report the calibration procedure and parameter bounds used in the applicable security model	Detector calibration[44]; source-intensity errors[143]; phase-reference attack[144]; one-time shot-noise calibration[145].
Networks and nodes	Multiuser TF-QKD; network trust and security; provider-network testbeds	Distinguish topology, tested user count, simultaneous links and operational assumptions	Network-security challenges[131]; provider testbed[133]; multiuser TF-QKD[134]; CV trust levels[146].
Heterogeneous channels	Free-space CV-QKD; daylight integrated QKD; satellite and space-to-ground links	State the protocol and channel conditions; separate demonstrations from feasibility analyses	Space-to-ground demonstrations[7,8]; daylight integrated link[110]; free-space phase compensation[147]; CV-MDI channel analysis[148].
Related integrated technologies	Integrated QKD/QRNG; orbital-angular-momentum multiplexing; multiuser quantum networks	Identify the function and application metric supported by each technology	OAM multiplexing[85]; multiuser network[86]; QKD/QRNG integration[137]; chip QRNG[149].
Receiver and digital processing	Local-oscillator phase compensation; PSK modulation; practical homodyne modeling	State local-oscillator architecture, modulation, receiver model and processing assumptions	Local-oscillator phase compensation[150,151]; PSK/QPSK[152,153]; homodyne model[154].

CV-QKD: continuous-variable QKD; TF-QKD: twin-field QKD; QRNG: quantum random number generation; PSK: phase-shift keying; OAM: orbital angular momentum; QPSK: quadrature phase-shift keying; CV-MDI: continuous-variable measurement-device-independent.

2. Protocol Requirements and Device-Level Constraints for Integrated Photonic QKD Chips

As QKD moves from experimental links to deployable systems, integrated photonic chips must translate protocol assumptions into device-level metrics. The relevant question is not only how many optical functions can be integrated. It is which constraints on state preparation, encoding, synchronization, interference, coherent measurement and monitoring must be preserved in hardware. Figure 2 compares the relative stringency of chip-level requirements across representative QKD protocols and encoding approaches. Higher scores indicate more stringent requirements in the corresponding dimension; for optical loss, this means a stronger requirement to minimize loss. The qualitative scores summarize the engineering requirements discussed in Section 2, while Table 1 specifies the corresponding protocol assumptions and trust boundaries. At a fundamental level, these constraints arise from quantum-state preparation, the role of loss and noise in the secret-key rate, and the mapping of receiver outcomes onto the security model[1-3,30]. An integrated QKD chip should therefore be regarded as a protocol-constrained quantum photonic system, not as a generic optical-communication component[3,24,29].

BB84 and decoy-state protocols provide the baseline case. Lo, Ma and Chen introduced decoy-state QKD to estimate the single-photon contribution from weak coherent pulses with different mean photon numbers, enabling practical sources to resist photon-number-splitting attacks[19]. Wang independently formulated a decoy-state method for defeating the same attack class, reinforcing the importance of source photon-number control[20]. At the chip level, this means that transmitters must provide intensity modulation while preserving decoy intensity, phase randomization, spectral shape and spatial mode within the security model. If modulators or attenuators introduce distinguishable temporal, spectral, polarization or spatial signatures, an adversary may obtain side information about state preparation[3,21,29].

The representative system layouts collected in Figure 3 are drawn from three experimentally important routes: high-speed silicon-photonic discrete-variable QKD (DV-QKD), chip-based MDI-QKD and composable-security CV-QKD demonstrations[31-33]. This comparison clarifies why phase-encoded and time-bin protocols impose direct constraints on integrated interferometers. Their key rates depend on interference visibility, phase error, path-length matching, thermal drift and polarization-dependent loss. PLC, silicon photonic and related waveguide platforms can integrate unbalanced Mach-Zehnder interferometers (MZIs), delay lines and phase

modulators on the same chip, thereby improving relative path stability[11,12,29]. Chip designs for phase-encoded QKD must therefore co-optimize low loss, low polarization-dependent loss, thermal tuning range, phase-control precision and online calibration.

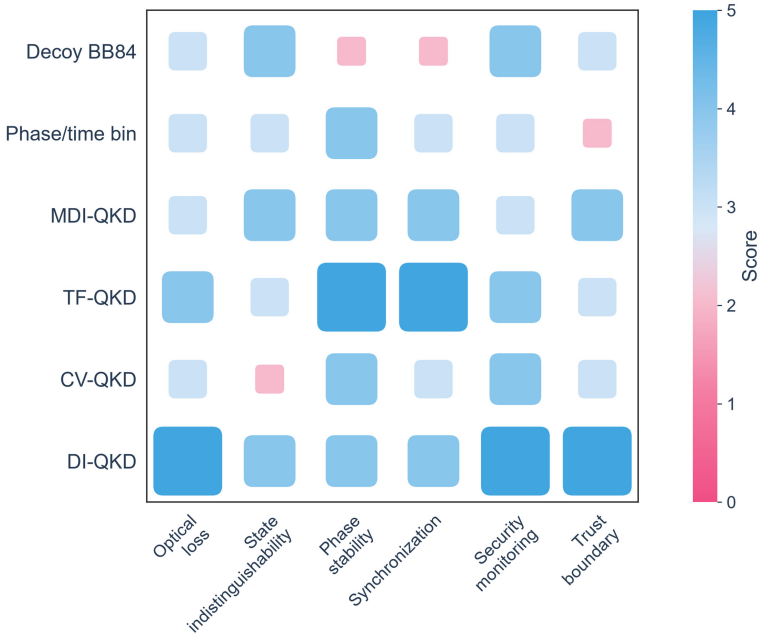


Figure 2. Protocol- and encoding-dependent requirements for integrated photonic QKD chips. The six columns compare optical loss, state indistinguishability, phase stability, synchronization, security monitoring and trust boundary. Colors and marker sizes indicate qualitative scores on a 0-5 scale, with higher scores denoting more stringent requirements. For optical loss, higher scores indicate a stronger requirement to minimize loss. The trust-boundary scores indicate the stringency of requirements for defining and maintaining the relevant trust assumptions. Scores summarize the authors' qualitative assessment of representative implementations discussed in Section 2 and Table 1. QKD: quantum key distribution.

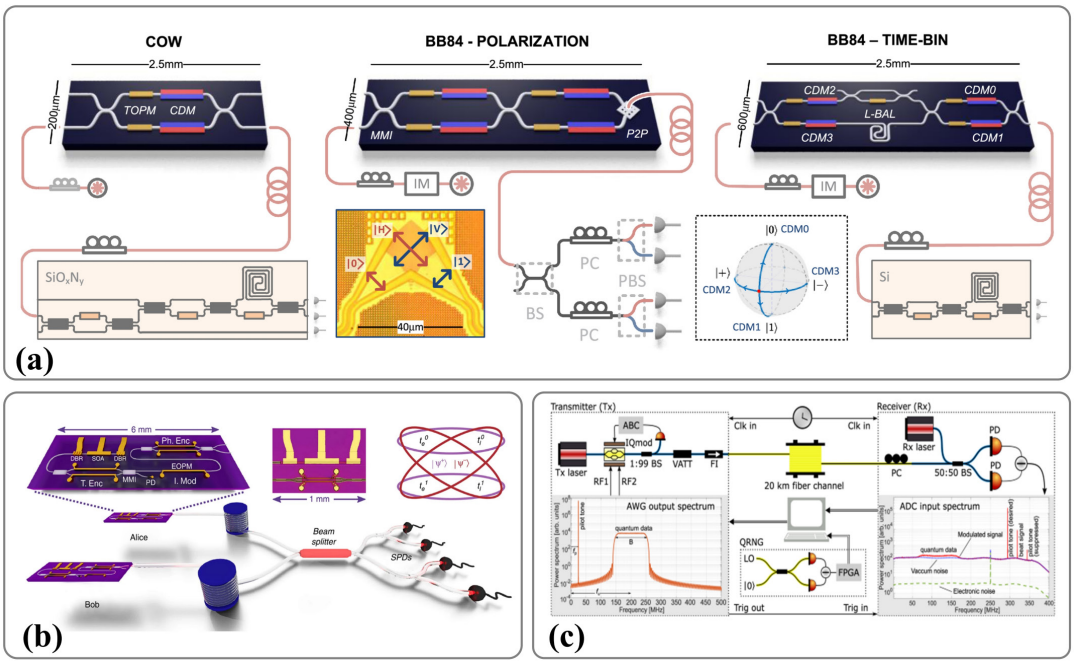


Figure 3. Representative QKD system architectures and their chip-level implications. (a) From left to right: COW, polarization-encoded BB84 and time-bin BB84 layouts highlight source preparation and interferometric stability requirements. Reproduced from reference[31]. CC BY 4.0; (b) MDI-QKD shifts the trusted boundary away from the measurement unit and makes independent-user indistinguishability central. Reproduced from reference[32]. CC BY 4.0; (c) CV-QKD relies on coherent detection, shot-noise calibration and receiver linearity. Reproduced from reference[33]. CC BY 4.0. QKD: quantum key distribution; COW: coherent-one-way; MDI-QKD: measurement-device-independent QKD; CV-QKD: continuous-variable QKD.

The three panels also identify different subsystem boundaries. In the discrete-variable (DV) layouts, the chip must prepare the intended intensity and encoded states, while any interferometric receiver must preserve the required path delay and visibility[31]. In MDI-QKD, two user transmitters must deliver compatible states to an untrusted measurement station[32]. In CV-QKD, the central requirements are modulation fidelity, coherent detection, and calibrated noise estimation; Figure 3c illustrates these system requirements and should not be interpreted as a fully integrated chip implementation[33]. Coherent-one-way (COW) monitoring and phase-randomized decoy-state BB84 use different coherence assumptions, so their source specifications cannot be interchanged simply because both employ time-resolved optical circuits[31].

MDI-QKD changes the security boundary. Lo, Curty and Qi placed the measurement unit outside the trusted boundary, removing detector side channels from the direct assumptions of the security proof[22]. Braunstein and Pirandola similarly emphasized the importance of eliminating measurement-device trust assumptions[23]. For integrated chips, this moves the key device metric from receiver detector characterization to indistinguishability between independent user transmitters. Wei demonstrated high-speed MDI-QKD with integrated silicon photonics, and Semenenko reported chip-based MDI-QKD, showing that multi-user interference can be implemented with compact photonic circuits[32,34].

For chip-based DV-MDI-QKD, the design specification should therefore report pulse timing and width, spectral detuning, polarization alignment and spatial-mode overlap, together with the source-intensity settings and their uncertainties. These quantities affect two-photon interference and the detection statistics used for decoy-state estimation[22,32,34]. Interference visibility must be reported with the input-state and background-subtraction conventions, rather than treated as a universal security threshold. Source characterization, private randomness and authenticated classical communication remain necessary even when the measurement station is untrusted[3,22]. In particular, polarization-dependent loss can make the emitted states basis dependent; a recent two-chip experiment explicitly incorporated this imperfection into MDI-QKD key-rate estimation and demonstrated transmission over 202 km[35].

TF-QKD and sending-or-not-sending protocols shift the long-distance problem from single-link attenuation to remote phase reference and interference stability. Lucamarini proposed TF-QKD to overcome the linear rate-transmittance scaling of repeaterless quantum communication through single-photon interference[36]. Wang later reported TF-QKD over 830 km of fiber, and Liu pushed experimental TF-QKD to the 1,000 km scale[37,38]. These results indicate that chip-based TF-QKD transmitters must prioritize frequency stability, phase tracking, reference isolation and long-term interferometric reproducibility.

CV-QKD is closely connected to coherent optical communication. The coherent-state protocol of Grosshans and Grangier, together with Gaussian-modulated coherent-state experiments, linked QKD to homodyne and heterodyne detection[39,40]. Qi introduced a local local-oscillator (LLO) approach that reduces engineering dependence on transmitting a strong local oscillator, and Jain demonstrated practical CV-QKD with composable security[25,33]. Integrated CV-QKD depends on linear modulators, balanced coherent receivers, shot-noise calibration, analogue bandwidth and digital signal processing, rather than on single-photon counting alone[41,42].

For CV-QKD, a receiver specification should state whether the local oscillator is transmitted or generated locally, the shot-noise normalization, the trusted detector parameters, and the calibration procedure[25,43,44]. Receiver bandwidth and symbol rate describe acquisition capability, not the final secret-key throughput. A reported rate must also be identified as asymptotic or finite-key and linked to the modulation and detection models used in the security analysis[33,45-47].

The protocol comparison in Table 1 further shows that trust boundaries are not interchangeable across QKD families. DI-QKD bases security on Bell nonlocality and minimal device trust, but current experiments remain constrained by detection efficiency, loss, finite-key effects and long-term stability[5,48]. MDI-QKD mainly removes detector-side assumptions, decoy-state BB84 constrains source photon-number statistics, and CV-QKD requires accurate modelling of excess noise and coherent detection[3,22,24,39]. The security design of integrated QKD chips cannot rely on a single universal metric. It must define trusted boundaries separately for the source, channel, measurement and control subsystems.

These protocol requirements constrain integrated photonic QKD chips in four ways. First, optical loss, crosstalk and mode distinguishability determine whether prepared states remain compatible with the protocol model. Second, modulation accuracy, phase stability and synchronization determine encoding quality. Third, receiver bandwidth, timing jitter and detector or homodyne noise determine measurement fidelity. Fourth, monitoring and calibration determine whether device parameters can be bounded during operation. The following sections therefore evaluate chip platforms and systems by their ability to satisfy protocol-specific constraints rather than by integration density alone.

3. Photonic Platforms and Integration Architectures

A photonic integrated chip denotes an optical circuit fabricated on a substrate; a chip-based QKD system combines one or more such circuits with the off-chip optics, electronics and processing needed to execute the protocol. Heterogeneous integration combines distinct material or device technologies, whereas a packaged module includes the optical, electrical and thermal interfaces required for operation[10,18,49].

Protocol constraints become deployable hardware only through material platforms, device blocks and transceiver architectures. The radar charts in Figure 4 compare the qualitative capabilities of representative photonic platforms and receiver integration routes in low-loss operation, modulation, integration, source/receiver integration and stability[3,10,29,50]. The same protocol can follow different implementation routes: silica PLCs favour low-loss and stable interferometry, silicon photonics supports dense complementary metal-oxide-semiconductor (CMOS)-compatible circuits, thin-film lithium niobate enables high-speed electro-optic modulation, and InP or hybrid platforms support active sources and detector interfaces[11,12,18,51].

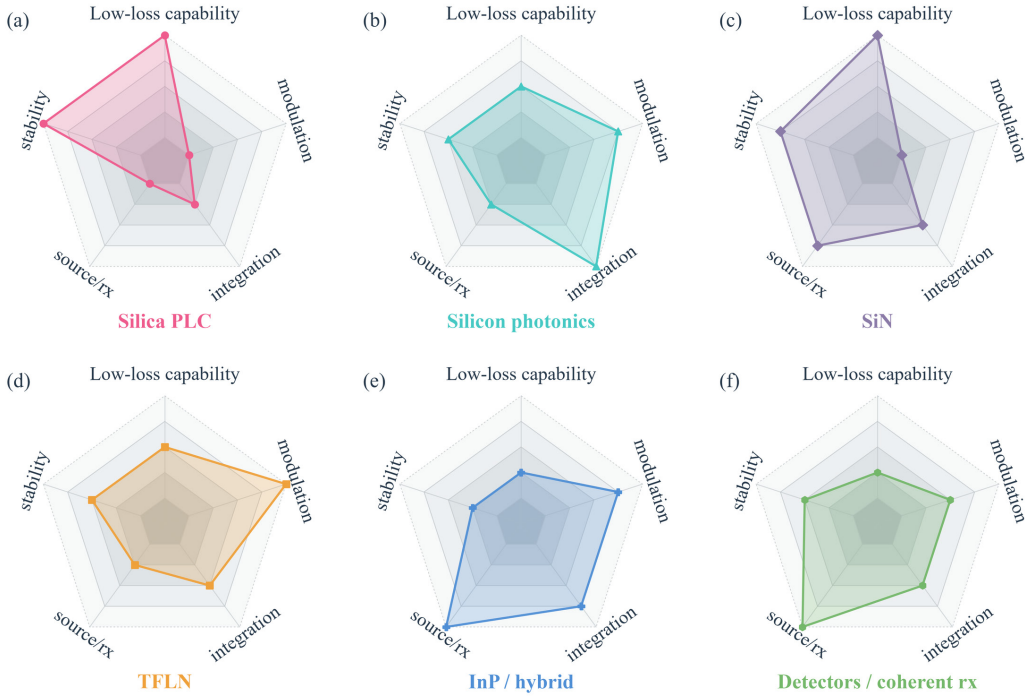


Figure 4. Qualitative capability profiles of representative photonic platforms and receiver integration routes for QKD. The radar charts compare low-loss capability, modulation capability, integration capability, source/receiver integration and stability. Larger radial values indicate stronger capability in the corresponding dimension on a five-level scale. The scores summarize the authors' qualitative assessment of representative implementations discussed in Section 3 and Table 2. Panels show (a) silica PLC; (b) silicon photonics; (c) SiN; (d) TFLN; (e) InP/hybrid integration; and (f) detector/coherent-receiver integration. QKD: quantum key distribution; PLC: planar lightwave circuit; InP: indium phosphide; TFLN: thin-film lithium niobate.

Silica PLCs remain important because QKD interferometry benefits directly from fiber-compatible processing, low propagation loss, weak polarization sensitivity and long-term stability. Nambu, Hatanaka and Nakamura proposed a BB84 system based on silica PLCs, and Honjo used a PLC MZI for differential-phase-shift QKD[14,15]. Kimura demonstrated single-photon interference over 150 km using silica integrated-optic interferometers, confirming the value of PLC path stability in long-distance coherent interference[52]. Nambu, Yoshino and Tomita then moved PLCs toward practical encoder and decoder units[53]. These results explain why PLCs remain useful for phase-encoded, time-bin and polarization-insensitive receiver modules, even when active modulation is supplied by other platforms.

Silicon photonics provides a well-developed route to dense and scalable transceiver chips, and its development shows a clear progression from device physics to link-ready subsystems. The device basis was established early, with high-speed silicon modulation through carrier-dispersion effects and the positioning of silicon quantum photonics as a platform for integrated interference and state manipulation[54,55]. On this basis, chip-scale QKD links have been demonstrated, including high-speed silicon-photonic QKD, a composable secret-key rate of 157 kbit/s over a 43 km link at 16.4 dB loss, and a photonic integrated quantum secure communication system[12,31,56]. More recent silicon-electronic co-integration and CMOS-compatible silicon QKD chips extend this progression toward link-ready subsystems[57,58]. Integrated multiuser receiver architectures offer a complementary route to sharing detection resources[59].

Silicon nitride and thin-film lithium niobate fill complementary gaps. Silicon nitride offers low-loss routing, broad optical bandwidth and microresonator-based quantum light sources; this makes it suitable for delay lines, filters, frequency-bin resources and multiwavelength quantum photonics[60-64]. Thin-film lithium niobate adds strong Pockels-effect modulation. Wang demonstrated CMOS-compatible lithium-niobate electro-optic modulators, and He reported hybrid silicon-lithium-niobate MZI modulators for 100 Gbit/s and beyond[51,65]. These capabilities are directly relevant to decoy modulation, CV-QKD coherent-state preparation and TF-QKD phase control, provided that RF packaging, optical coupling and process uniformity are controlled.

InP, III-V/silicon and broader heterogeneous integration provide routes to active sources and multi-material functionality. Smit described InP generic integration, where lasers, semiconductor optical amplifiers, modulators and detectors can share a common platform[66]. Liang, Roelkens and Fathpour showed that III-V gain and silicon passive circuits can be combined to overcome single-platform limitations[67-69]. Hybrid integrated quantum photonics further suggests that sources, routing, modulation and detection can be assigned to materials according to function[49]. Table 2 condenses these trade-offs into device-level selection criteria for QKD chips, highlighting where each platform is naturally strong and where hybridization is likely to be necessary.

Platform comparisons must separate waveguide propagation loss, single-interface coupling loss and packaged insertion loss, because they describe different parts of the link budget. Reported values require a wavelength, waveguide geometry and measurement configuration; a best-case passive-waveguide result should not be treated as the loss of a complete QKD module[10,18,60,61]. Likewise, process maturity should be described through available fabrication processes, design tools, reproducibility and packaging evidence, rather than inferred from a single working device. Heterogeneous integration adds interface alignment, back-reflection and thermal-management constraints, so the benefit of combining materials must be assessed at module level[49,67-69].

Transmitter and receiver architectures convert those platform capabilities into protocol states and measurement outcomes. Figure 5 brings together device examples that span high-speed silicon-photonic MDI-QKD transmitters, modulator-free transmitter design, receiver integration and GHz-rate detector-integrated reception[34,50,70,76]. The comparison shows that an integrated QKD architecture is a closed measurement system, not a simple aggregation of optical blocks. Source interfaces, intensity, phase, polarization or time-bin encoding, attenuation, monitoring taps, decoding interferometers, filters, detector interfaces, coherent receivers and electronic control must be specified together[11-13,29]. Transmitter and receiver non-idealities jointly determine state-preparation error, measurement error, mode leakage, stability and the final secret-key rate[3,29].

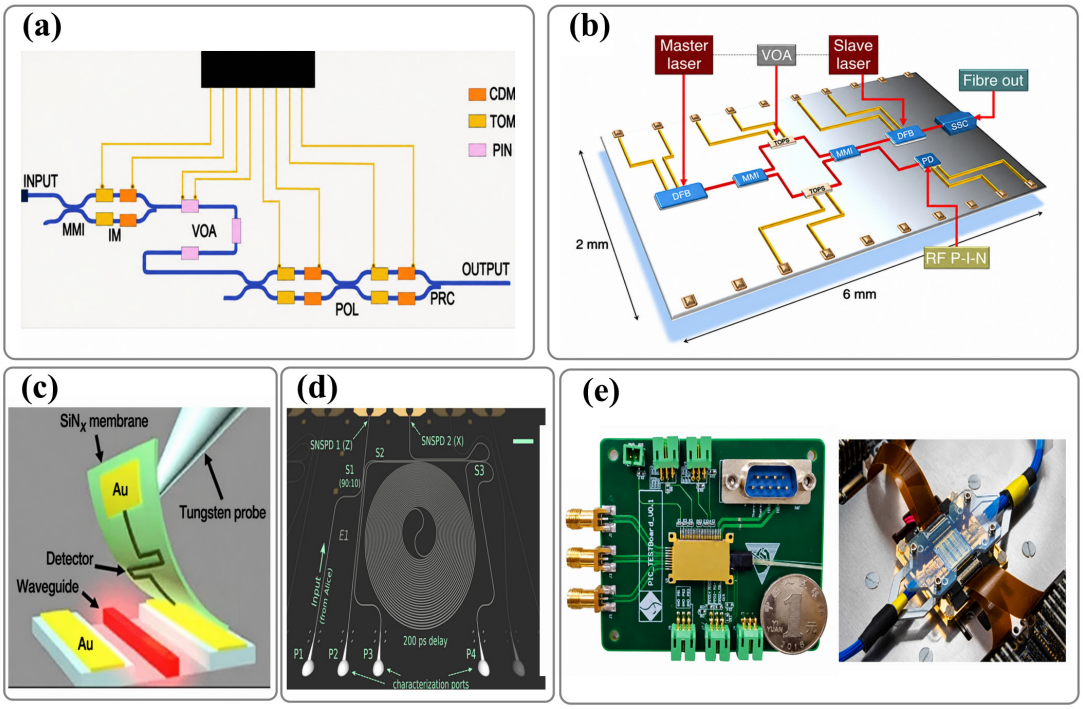


Figure 5. Representative transmitter and receiver implementations in integrated QKD. (a) Integrated silicon-photonic transmitter architecture for high-speed MDI-QKD, showing how modulation and interference preparation are brought onto chip. Reproduced from reference[34]. CC BY 4.0; (b) Modulator-free transmitter design, illustrating an alternative route that reduces high-speed external modulation. Reproduced from reference[70]. CC BY 4.0; (c) Transfer integration of a membrane-supported superconducting nanowire single-photon detector onto a photonic waveguide. The waveguide guides photons to the detector, gold contacts provide electrical connections for biasing and readout, and the tungsten probe positions the detector membrane during transfer. Reproduced from reference[50]. CC BY 4.0; (d) Optical micrograph of a detector-integrated on-chip QKD receiver. Reproduced from reference[76]. CC BY 4.0; (e) Packaged transmitter and receiver modules, emphasizing the transition from chip layout to deployable hardware. Reproduced from reference[34,50]. CC BY 4.0. QKD: quantum key distribution; MDI-QKD: measurement-device-independent QKD.

The transmitter chip maps protocol variables onto physical quantum states. In decoy-state BB84, the analyses by Lo, Ma and Chen and by Wang require weak coherent sources to switch among different mean photon numbers so that the single-photon contribution can be estimated[19,20]. At the chip level, this requirement couples high-speed intensity modulation, variable attenuation, phase randomization and monitoring taps. Paraïso reduced reliance on high-speed external modulators with a modulator-free transmitter chip, whereas Ma and Cai demonstrated silicon-photonic polarization-encoded transmitter and transceiver circuits[70,71,72]. These

designs show that transmitter miniaturization is useful only when drive calibration, decoy-state indistinguishability and monitoring are preserved.

Detector and coherent-receiver interfaces define the measurement side of the architecture, and the relevant figures of merit are detection efficiency, dark-count rate, timing jitter and, for coherent reception, bandwidth and linearity[73-75]. On the single-photon side, travelling-wave superconducting-nanowire single-photon detectors (SNSPDs) have been embedded in nanophotonic circuits, a detector-integrated on-chip QKD receiver has been operated at GHz clock rates, and a heterogeneously integrated superconducting silicon-photonic platform has been proposed for MDI-QKD[76,77,78]. On the coherent side, integrated photonic-electronic receivers now reach beyond 20 GHz for balanced detection and 9 GHz for squeezed-light measurement, and a 10 GBd (gigabaud) CV-QKD experiment with an integrated receiver estimated key rates of 0.737 Gbit/s over 5 km and 0.315 Gbit/s over 10 km, including finite-size parameter-estimation effects in its collective-attack analysis[41]. The broadband detector demonstrations establish receiver capability separately[79,80]. Chip-scale and time-domain homodyne detectors further show that bandwidth, linearity and shot-noise clearance are receiver-level rather than isolated photodiode metrics[81-83].

Chip architectures are also expanding beyond a single degree of freedom. High-dimensional QKD using multicore fiber and silicon photonic integrated circuits brought spatial encoding into an on-chip framework[84]. Orbital-angular-momentum multiplexing extends the spatial encoding options[85], while entanglement-based integrated multiuser networks demonstrate a distinct networking application[86]. These developments broaden the role of integrated QKD chips from compact BB84 transmitters to configurable quantum-communication nodes. The security challenge is that added degrees of freedom can also create added leakage channels, so monitoring and calibration must scale with architectural complexity.

4. Module Engineering, Calibration and Security-Parameter Mapping

A QKD chip becomes a deployable module only when its optical, electronic and thermal responses remain measurable and stable after packaging. Phase drift, thermal crosstalk, polarization drift, coupling loss, drive crosstalk and calibration bias enter state preparation, interference measurement, excess-noise estimation and the boundary of the security proof[3,4,29]. Bare-chip insertion loss, modulation bandwidth or detector efficiency therefore indicate device potential, but deployment value depends on whether the packaged module remains calibratable under temperature variation, vibration, ageing, fiber coexistence and unattended operation[10,17,18].

Phase stability is a common constraint for phase-encoded, time-bin, MDI-QKD, TF-QKD and CV-QKD chips. Sibson and Bunandar showed that shortened on-chip paths can support stable high-speed and metropolitan QKD, but these advantages depend on trackable phase response under modulation, tuning and package stress[11,12]. The silicon-photonic CV-QKD platform of Zhang and the high-speed integrated QKD system of Sax further show that phase compensation, drive synchronization and stable calibration must operate as part of the link, not as occasional offline adjustments[13,87]. Phase-remapping studies by Fung and Xu, together with calibration-security analysis by Jain, show that imperfect phase modulation can become an exploitable side channel if it is not bounded in the security model[88-90].

Thermal control and electro-optic modulation play different roles. Silicon thermo-optic phase shifters provide compact tuning for drift compensation, as demonstrated by Harris, but they are better suited to slow control than to carrying high-speed encoding[91]. Lithium-niobate and hybrid silicon-lithium-niobate devices use electro-optic modulation for high-speed phase and intensity control, with 100 Gbit/s-class demonstrations providing a device basis for high-rate QKD encoding and CV-QKD modulation[51,65].

Packaging must preserve polarization, coupling and monitoring fidelity. QKD is more sensitive than classical communication to polarization-dependent loss, polarization-mode dispersion and basis mismatch because these effects modify state distinguishability and measurement statistics[3,4]. Wang demonstrated an integrated dynamic polarization controller, Zhang reported polarization-insensitive QKD using PLC chips, and Choe implemented a compact 1 × 4 polarization beam-splitter module for free-space BB84 reception[16,92,93]. These studies indicate that package design should be treated as a security-relevant part of the optical system, not as a final mechanical step.

These effects enter security analysis through different observables. Phase drift changes interference statistics and, in CV-QKD, contributes to the inferred phase-noise budget; polarization-dependent loss changes transmission in a state-dependent manner[35,43,94]. Thermal or electrical crosstalk should be characterized under simultaneous channel operation, since a calibration of isolated components need not bound correlated preparation errors. We recommend reporting the measurement interval, environmental conditions and uncertainty alongside each security-relevant parameter, and verifying that the resulting bounds remain valid during key acquisition.

Control electronics and calibration strategies must be designed together with the protocol model. Yuan's directly phase-modulated light source reduces the conventional modulation chain, but it requires accurate modelling of source dynamics[95]. For MDI-QKD, polarization-multiplexing and phase-reference-free schemes reduce calibration burden, while CV-QKD LLO and self-coherent reference-sharing schemes move phase handling into receiver estimation and compensation[96-98]. Local-oscillator phase attacks and

phase-noise models identify requirements for the phase-reference treatment[43,99]. Receiver imbalance, shot-noise calibration and trusted detector-noise studies address distinct receiver assumptions[44,100,101]. We recommend recording the corresponding calibration bounds and using them consistently in key-rate estimation.

Reliability evaluation should expand from device metrics to module-level and security-level metrics. Photonic packaging usually emphasizes coupling loss, bandwidth, thermal resistance and mechanical robustness. QKD modules also require records of phase error, extinction-ratio drift, decoy-intensity drift, polarization-dependent loss, monitoring-tap stability, detector-gating drift, excess-noise bias and confidence intervals for calibration parameters[3,29,88,102]. Practical security analyses of chip-based CV-QKD and CV-QKD with imperfect phase-reference calibration show that device imbalance, noise modelling and calibration cannot be treated as ordinary engineering imperfections[94,100,102].

Acceptance limits must be distinguished from representative device specifications. A quoted extinction ratio, visibility or noise value is not a protocol-independent guarantee of security. The admissible range depends on the source and detector models, channel loss, observed statistics, block size and security parameters[3,33,46,103]. For decoy-state operation, photon-number statistics and finite-key estimation must be consistent with the characterized source[19,20,104]. For CV protocols, the shot-noise calibration and the treatment of trusted detector noise must match the security model[44,47,101].

Representative numbers illustrate why these categories must remain separate. A 20-mm thin-film lithium-niobate modulator reported a half-wave voltage of 1.4 V, an electro-optic 3-dB bandwidth above 45 GHz and on-chip optical loss below 0.5 dB[51]; these are device specifications, not a demonstrated QKD security limit. A silicon-photonic MDI-QKD experiment measured Hong-Ou-Mandel visibility up to 48.4% and obtained a finite-key rate of 31 bit/s at 36 dB channel loss[34]. That visibility was an operating result for the stated sources and measurement configuration, not a universal acceptance threshold. For a particular module, an acceptance test should instead propagate the measured uncertainty intervals into the chosen key-length calculation and require a positive lower bound at the declared security level and operating loss.

Network coexistence adds another reliability boundary. Karinou discussed routes toward integrating CV-QKD into deployed optical networks, and Kumar studied coexistence between CV-QKD and intense dense wavelength-division multiplexed (DWDM) classical channels[105,106]. DWDM crosstalk studies examine coexistence-induced noise[107], while upstream CV-QKD access experiments address a distinct network configuration[108]. Reconciliation methods contribute another processing constraint on the achieved throughput[109]. These topics should be evaluated separately when specifying synchronization, noise control and classical-channel isolation. Packaged QKD chips should therefore report packaged insertion loss, environmental drift, calibration interval, coexistence conditions and security-parameter traceability.

5. Chip-Based QKD System Demonstrations and Network Deployment

System experiments are the point where protocol assumptions, chip metrics, package stability, synchronization, post-processing throughput and network conditions become inseparable. Table 3 summarizes representative link results and identifies their integration scope or comparison boundary. Metropolitan, satellite and space-to-ground demonstrations show that QKD can operate in multi-node and cross-domain infrastructures, but they also expose the size, interconnection, maintenance and calibration burden of discrete optical systems[6–9]. Integrated chips address this burden only if packaging, control and security monitoring remain stable during operation.

Discrete-variable chip-based systems first showed that integrated transmitters and receivers can carry real protocol functions. Integrated transmitter encoding has been realized on a photonic chip; a metropolitan link delivered 157 kbit/s over 43 km at 16.4 dB loss; and a 1,550 nm silicon-photonic transmitter supported daylight free-space QKD over 145 m at a quantum bit error rate (QBER) of ~0.5% and a ~30 kbit/s average secret-key rate[11,12,110]. Chip-based QKD has since been pushed toward high-speed operation, including 2.5-GHz silicon-photonic system demonstrations[87,111]. The deployment examples in Figure 6 matter because they test chip functions under field conditions, including fiber loss, daylight background, calibration stability and link-level key extraction.

Differences in Table 3 cannot be attributed to chip material alone. Detection technology, clock or symbol rate, coupling and channel attenuation, modulation format, data-block size, reconciliation assumptions and offline versus real-time processing all affect the reported throughput. Integrated CV receiver estimates should therefore be compared with other estimates using compatible noise and security models, whereas composable DV results require their stated finite-key conditions.

Chip-based MDI-QKD experiments emphasize reproducibility of multi-user interference. Wei demonstrated high-speed MDI-QKD with integrated silicon photonics, and Semenenko demonstrated chip-based MDI-QKD, moving transmitter and Bell-state-measurement functions toward compact implementations[32,34]. Cao's integrated silicon-photonic MDI-QKD system further supports the view that stable two-photon interference, rather than device count alone, is the central metric for multi-user QKD nodes[112]. For deployed MDI-QKD, the relevant operating quantity is long-term indistinguishability of independent user pulses in timing, frequency, polarization and optical mode, together with stable protocol-dependent intensity and encoding settings.

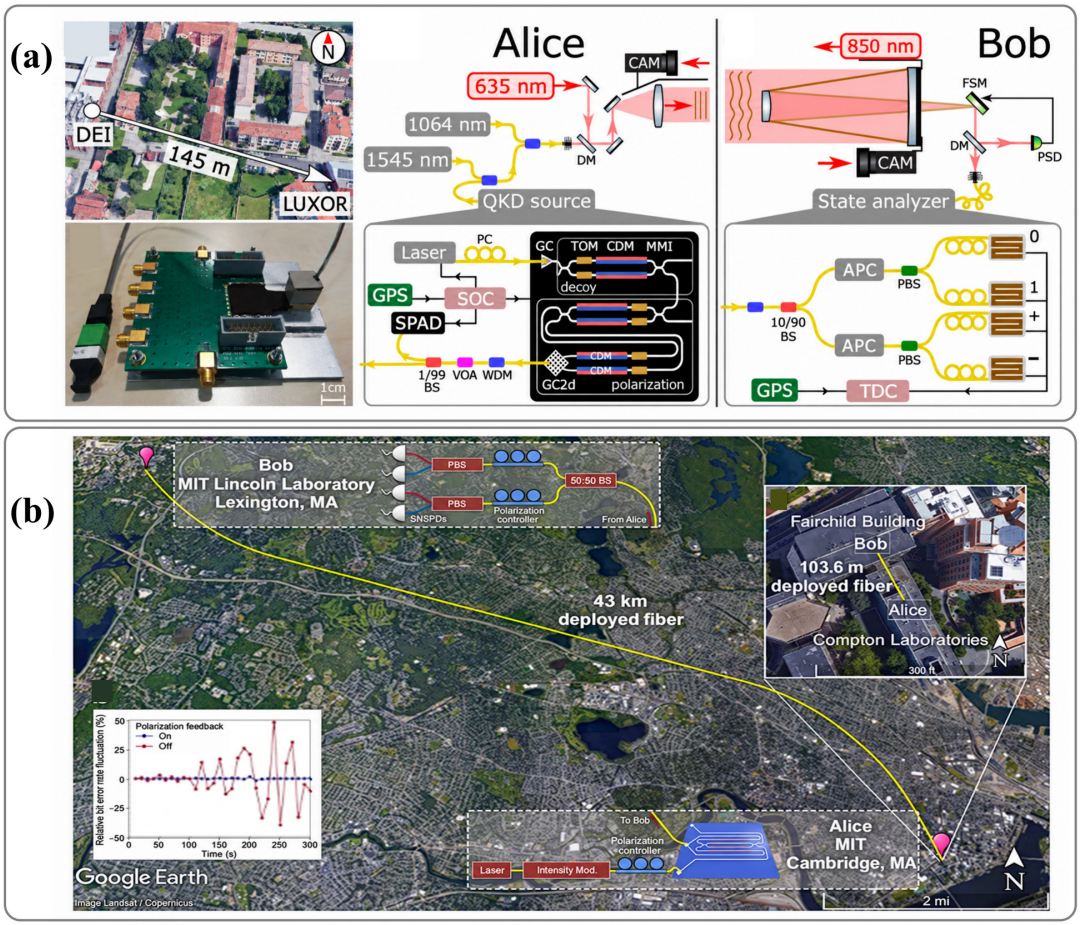


Figure 6. Field-oriented demonstrations of silicon-photonic QKD. (a) Daylight free-space implementation using a 1,550 nm silicon-photonic transmitter, illustrating compact terminal operation under background-light noise. Reproduced from reference[110]. CC BY 4.0; (b) Metropolitan field test over a 43 km dark-fiber link, showing how chip-based encoding can be evaluated in a realistic loss and calibration environment. Reproduced from reference[12]. CC BY 4.0. QKD: quantum key distribution.

CV-QKD system experiments shift the integration problem toward coherent modulation, balanced detection and photonic-electronic reception. Coherent modulation and receiver structures have been integrated on silicon photonics, a 10 GBd CV-QKD experiment has used an integrated receiver with offline digital processing, CV-QKD has been realized with on-chip light sources, and a silicon-photonic CV-QKD receiver platform has been reported[13,41,113,114]. In parallel, long-distance CV-QKD over 202.81 km highlights the importance of excess-noise control and phase compensation for distance extension[42]. These results show that CV-QKD chips must be evaluated by receiver bandwidth, shot-noise calibration, electronic noise, DSP complexity and secure throughput together.

Recent demonstrations further separate integration scope from the reported security regime. A PLC-module experiment combined a one-decoy method with advantage distillation at 625 MHz, reporting composable secret-key rates of 3.32 Mbit/s at 2 dB loss and 1.85 kbit/s at 18 dB loss[115]. A silicon-photonic transmitter–receiver implementation using 8-PSK modulation operated at 1.5625 GBd and reported asymptotic secret-key rates of 31.05 Mbit/s over 25.8 km and 5.05 Mbit/s over 50.4 km[116]. A further integrated CV-QKD demonstration reported an average 0.737 Mbit/s over 50 km during 12 h of operation, with the laser remaining external[117]. These examples illustrate complementary progress in post-processing, integrated coherent operation and stabilization.

Resource-efficient silicon-photonic BB84 also demonstrates how synchronization and polarization compensation can share the encoding and measurement resources, reducing auxiliary hardware requirements[118]. Chip integration extends to related cryptographic applications: a three-node quantum-digital-signature network used integrated encoding and decoding over distances up to 200 km[119].

Networked and high-rate QKD benchmarks prevent overinterpretation of chip integration. Discrete systems have reported high-rate QKD exceeding 110 Mbit/s, high secret-key-rate operation enabled by fast single-photon detectors and real-time key distillation, and fiber QKD over 307 km and 421 km[120-123]. Chip-based QKD may not immediately set every record for rate or distance, but it offers opportunities to improve module size, stability, manufacturing consistency and maintainability.

Network experiments now provide more direct evidence of scalability. An optical-frequency-comb MDI network reported an average

267 bit/s per user pair at approximately 30 dB link attenuation and demonstrated simultaneous communication between two pairs[124]. An integrated-photonic TF-QKD network used 20 client transmitter chips and a server microcomb chip, with sequential pairwise demonstrations through ten wavelength channels over 370 km of spooled fiber[125]. Recent long-distance photonic-integrated and microcomb-driven fully connected network studies extend this direction[126,127].

6. Practical Security and Shared Research Challenges

6.1 Practical Security and Evaluation Criteria

Practical security remains a design principle for future chip systems. Detector-blinding, time-shift and local-oscillator studies identify exploitable differences between physical devices and assumed detector or calibration models[26-28,128]. Trojan-horse bounds and loss-tolerant source analyses address complementary source-side risks[103,129]. The systems highlighted in Figure 7 build on two complementary lines of work: protocol-compatible chip-based QKD integration and high-dimensional silicon-photonic QKD using multicore fiber[11,84]. Together they show why future chips should expose measurable quantities for on-chip reflection, residual modulation, thermal crosstalk, polarization-dependent loss, monitoring-tap stability and package feedback, so that security proofs can use measured module parameters rather than idealized component assumptions.

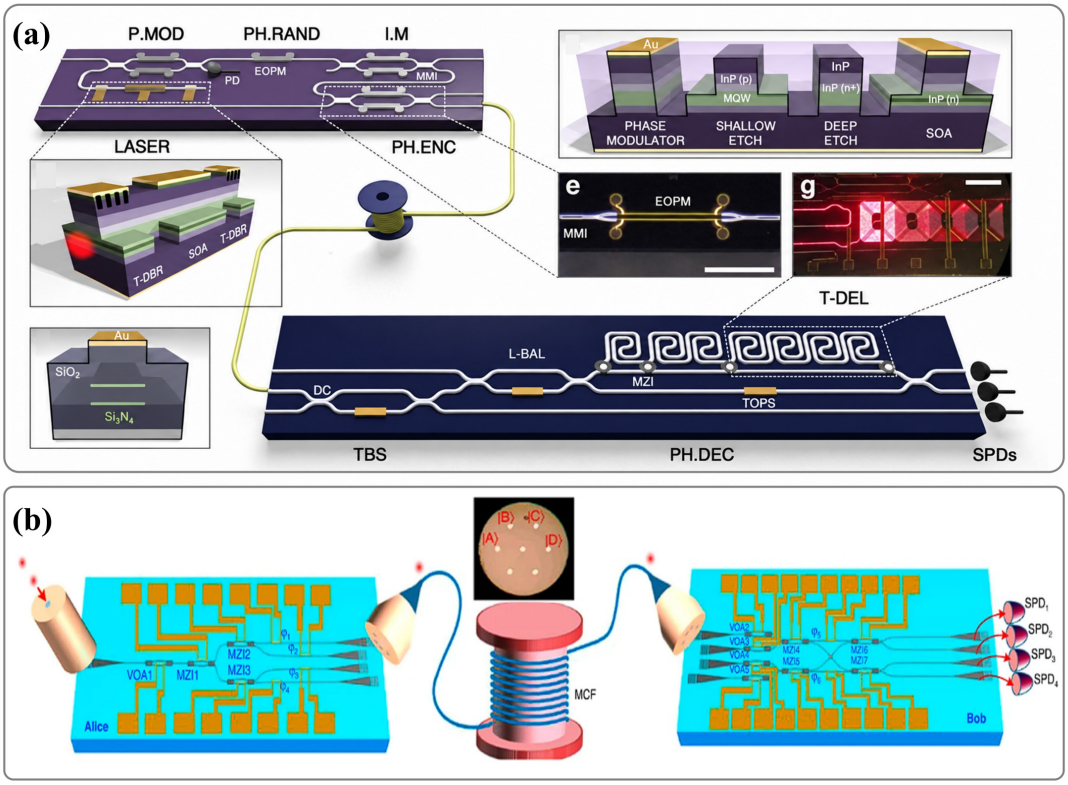


Figure 7. Integrated QKD architectures viewed through a practical-security lens. (a) Multi-protocol-compatible system using an integrated InP encoder and a Si_xN_y decoder, illustrating how heterogeneous integration can support protocol flexibility. Reproduced from reference[11]. CC BY 4.0; (b) Silicon photonic integrated circuit for noise-resistant high-dimensional QKD, showing how spatial encoding can extend the chip design space while introducing new calibration requirements. Reproduced from reference[84]. CC BY 4.0. QKD: quantum key distribution; InP: indium phosphide.

Chip-specific modulation physics introduces additional tests. Kang *et al.* demonstrated that externally injected femtosecond pulses can exploit two-photon absorption in silicon photonic modulators to change emitted decoy intensities, causing legitimate users to overestimate the key rate under the uncorrected model[130]. This is a concrete example of a material-level mechanism affecting a security-relevant source parameter. Isolation and monitoring must therefore be evaluated over the relevant injection conditions, and their residual bounds must be included in the source model; integration alone does not establish resistance to such perturbations.

6.2 Shared challenges and future directions

Future QKD networks will require chip modules that can coexist with classical infrastructure and network management. QKD network-security studies discuss operational and trust challenges[131,132], while provider-network testbeds investigate integration into existing infrastructure[133]. Untrusted-relay MDI and TF networks address specific measurement-station trust assumptions[124,125,134]; they should not be conflated with arbitrary trusted-node-free routing. Satellite-to-ground and integrated space-to-ground

demonstrations provide a separate class of deployment evidence[7,8]. Integrated chips should therefore be assessed not only by peak key rate, but also by pluggable interfaces, remote calibration, power consumption, environmental retention, compatibility with network control and traceability of security parameters.

Artificial intelligence (AI) may provide an additional control and monitoring layer for future chip-based QKD networks. By learning from optical, electrical, thermal and protocol-level telemetry, AI-assisted systems could automatically identify abnormal patterns associated with hacking attempts, side-channel exploitation and device imperfections, including unexpected phase drift, modulation errors, polarization-dependent loss, thermal crosstalk and detector anomalies. In parallel, real-time AI-based resource management could optimize channel allocation, wavelength assignment, routing, key-pool utilization, power consumption and calibration schedules, while dynamically configuring quantum communication networks in response to changing traffic loads, link conditions and security risks. Such functions should be implemented as security-aware decision-support mechanisms rather than as substitutes for composable security proofs. Their training data, false-positive and false-negative rates, response latency, robustness against adversarial manipulation and interaction with the trusted boundary must be explicitly characterized. Any AI-driven reconfiguration should also be auditable and constrained by predefined security policies, so that network optimization does not introduce unmodelled side channels or invalidate the assumptions used in key-rate estimation[135,136].

At the platform level, one promising route is heterogeneous integration combined with security-oriented co-design. No single material platform easily provides low loss, high-speed modulation, on-chip sources, detector interfaces and low-cost packaging at the same time[17,49]. Integrated QKD and quantum random number generation (QRNG) technologies, hybrid silica-lithium-niobate transmitter chips, silica-silicon PLC decoding chips and polarization-based silicon encoder-decoder chips indicate that practical systems will allocate functions across materials and packages[137-140]. A QKD chip specification should thus include low-loss passive routing, low-voltage modulation, low-noise reception, on-chip monitoring, thermal management, calibration logging and an explicit mapping from measured parameters to security assumptions.

Beyond the platform and network directions above, a further group of recent security, protocol and integrated-photonics studies is best read as a set of evaluation dimensions that a chip specification should report explicitly. Table 4 consolidates these dimensions, the evidence each line of work establishes, and the corresponding requirement on the chip specification, while distinguishing published evidence from proposed reporting practices. These recommendations do not constitute a validated certification standard.

The remaining challenges are shared across material and protocol choices. First, the useful loss budget includes propagation, coupling, filtering and monitoring losses after packaging, not only the best passive-waveguide value[10,18]. Second, a reproducible module requires stable calibration across devices and operating conditions; wafer-scale and network demonstrations provide evidence beyond a single optimized chip[125]. Third, integration must be evaluated together with the remaining laser, detector, control-electronic and digital-processing resources[41,49]. We recommend reporting these resources, operating duration, calibration intervals and parameter uncertainties alongside the secret-key rate. DI-QKD security studies and multiuser TF-QKD architectures motivate longer-term research, but their assumptions and level of experimental implementation must be distinguished[48,134].

7. Conclusion

This review has summarized the protocol requirements, material platforms, integrated devices and system demonstrations of chip-based QKD. Complementary advances in silicon, silicon nitride, silica, thin-film lithium niobate and InP have enabled compact transmitters and receivers, with progress extending to metropolitan links and multi-user networks. Secure-key performance depends on accurate state preparation, low optical loss, stable interference and well-characterized detection, together with reliable synchronization and post-processing. Further development of heterogeneous integration, packaging, automated calibration and photonic–electronic co-design will help translate these advances into scalable and maintainable QKD modules for quantum-secure communication networks.

Declarations

Acknowledgements

GPT-5.6 was used during preparation of the original manuscript for language polishing and for generating icon elements in conceptual illustrations (Figure 1).

Authors contribution

You J: Conceptualization, investigation, writing-original draft.
Yin X: Visualization, writing-review & editing.
Yang S: Formal analysis, methodology.
Hu C: Investigation.
Cheng P: Project administration, funding acquisition.

An J: Supervision, project administration, funding acquisition.

Conflicts of interest

The authors declare no conflicts of interest.

Ethical approval

Not applicable.

Consent to participate

Not applicable.

Consent for publication

Not applicable.

Availability of data and materials

Not applicable.

Funding

This work has been supported by Quantum Science and Technology-National Science and Technology Major Project (Grant No. 2021ZD0300701).

Copyright

© The Author(s) 2026.

References

1. Bennett CH, Brassard G. Quantum cryptography: Public key distribution and coin tossing. Theor Comput Sci. 2014;560:7-11. [DOI]
2. Scarani V, Bechmann-Pasquinucci H, Cerf NJ, Dušek M, Lütkenhaus N, Peev M. The security of practical quantum key distribution. Rev Mod Phys. 2009;81(3):1301-1350. [DOI]
3. Xu F, Ma X, Zhang Q, Lo HK, Pan JW. Secure quantum key distribution with realistic devices. Rev Mod Phys. 2020;92(2):025002. [DOI]
4. Diamanti E, Lo HK, Qi B, Yuan Z. Practical challenges in quantum key distribution. npj Quantum Inf. 2016;2:16025. [DOI]
5. Portmann C, Renner R. Security in quantum cryptography. Rev Mod Phys. 2022;94(2):025008. [DOI]
6. Sasaki M, Fujiwara M, Ishizuka H, Klaus W, Wakui K, Takeoka M, et al. Field test of quantum key distribution in the Tokyo QKD Network. Opt Express. 2011;19(11):10387-10409. [DOI][PubMed]
7. Liao SK, Cai WQ, Liu WY, Zhang L, Li Y, Ren JG, et al. Satellite-to-ground quantum key distribution. Nature. 2017;549(7670):43-47. [DOI]
8. Chen YA, Zhang Q, Chen TY, Cai WQ, Liao SK, Zhang J, et al. An integrated space-to-ground quantum communication network over 4,600 kilometres. Nature. 2021;589(7841):214-219. [DOI]
9. Dynes JF, Wonfor A, Tam WW, Sharpe AW, Takahashi R, Lucamarini M, et al. Cambridge quantum network. npj Quantum Inf. 2019;5:101. [DOI]
10. Wang J, Sciarrino F, Laing A, Thompson MG. Integrated photonic quantum technologies. Nat Photonics. 2020;14(5):273-284. [DOI]
11. Sibson P, Erven C, Godfrey M, Miki S, Yamashita T, Fujiwara M, et al. Chip-based quantum key distribution. Nat Commun. 2017;8:13984. [DOI]
12. Bunandar D, Lentine A, Lee C, Cai H, Long CM, Boynton N, et al. Metropolitan quantum key distribution with silicon photonics. Phys Rev X. 2018;8(2):021009. [DOI]
13. Zhang G, Haw JY, Cai H, Xu F, Assad SM, Fitzsimons JF, et al. An integrated silicon photonic chip platform for continuous-variable quantum key distribution. Nat Photonics. 2019;13(12):839-842. [DOI]
14. Nambu Y, Hatanaka T, Nakamura K. BB84 quantum key distribution system based on silica-based planar lightwave circuits. Jpn J Appl Phys. 2004;43(8B):L1109. [DOI]
15. 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(23):2797-2799. [DOI]
16. Choe JS, Ko H, Choi BS, Kim KJ, Youn CJ. Silica planar lightwave circuit based integrated 1 × 4 polarization beam splitter module for free-space BB84 quantum key distribution. IEEE Photonics J. 2018;10(1):7600108. [DOI]
17. Pelucchi E, Fagas G, Aharonovich I, Englund D, Figueroa E, Gong Q, et al. The potential and global outlook of integrated photonics for quantum technologies. Nat Rev Phys. 2022;4(3):194-208. [DOI]
18. Moody G, Sorger VJ, Blumenthal DJ, Juodawlkis PW, Loh W, Sorace-Agaskar C, et al. 2022 Roadmap on integrated quantum photonics. J Phys Photonics. 2022;4(1):012501. [DOI]

19. Lo HK, Ma X, Chen K. Decoy state quantum key distribution. Phys Rev Lett. 2005;94(23):230504. [DOI][PubMed]
20. Wang XB. Beating the photon-number-splitting attack in practical quantum cryptography. Phys Rev Lett. 2005;94(23):230503. [DOI] [PubMed]
21. Brassard G, Lutkenhaus N, Mor T, Sanders BC. Limitations on practical quantum cryptography. Phys Rev Lett. 2000;85(6):1330-1333. [DOI][PubMed]
22. Lo HK, Curty M, Qi B. Measurement-device-independent quantum key distribution. Phys Rev Lett. 2012;108(13):130503. [DOI]
23. Braunstein SL, Pirandola S. Side-channel-free quantum key distribution. Phys Rev Lett. 2012;108(13):130502. [DOI][PubMed]
24. Zhang Y, Bian Y, Li Z, Yu S, Guo H. Continuous-variable quantum key distribution system: Past, present, and future. Appl Phys Rev. 2024;11:011318. [DOI]
25. Qi B, Lougovski P, Pooser R, Grice W, Bobrek M. Generating the local oscillator "locally" in continuous-variable quantum key distribution based on coherent detection. Phys Rev X. 2015;5(4):041009. [DOI]
26. 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(10):686-689. [DOI]
27. Zhao Y, Fung CF, Qi B, Chen C, Lo HK. Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems. Phys Rev A. 2008;78(4):042333. [DOI]
28. Ma XC, Sun SH, Jiang MS, Liang LM. Local oscillator fluctuation opens a loophole for Eve in practical continuous-variable quantum-key-distribution systems. Phys Rev A. 2013;88(2):022339. [DOI]
29. Liu Q, Huang Y, Du Y, Zhao Z, Geng M, Zhang Z, et al. Advances in chip-based quantum key distribution. Entropy (Basel). 2022;24(10):1334. [DOI][PubMed][PMC]
30. Ekert AK. Quantum cryptography based on Bell's theorem. Phys Rev Lett. 1991;67(6):661-663. [DOI][PubMed]
31. Sibson P, Kennard JE, Stanisic S, Erven C, O'Brien JL, Thompson MG. Integrated silicon photonics for high-speed quantum key distribution. Optica. 2017;4(2):172-177. [DOI]
32. Semenenko H, Sibson P, Hart A, Thompson MG, Rarity JG, Erven C. Chip-based measurement-device-independent quantum key distribution. Optica. 2020;7(3):238. [DOI]
33. Jain N, Chin HM, Mani H, Lupo C, Nikolic DS, Kordts A, et al. Practical continuous-variable quantum key distribution with composable security. Nat Commun. 2022;13(1):4740. [DOI][PubMed][PMC]
34. Wei K, Li W, Tan H, Li Y, Min H, Zhang WJ, et al. High-speed measurement-device-independent quantum key distribution with integrated silicon photonics. Phys Rev X. 2020;10(3):031030. [DOI]
35. Zhu J, Ding H, Zhou X, Zhang C, Zhang C, Li J, et al. Chip-based measurement-device-independent quantum key distribution in the presence of polarization-dependent loss. Phys Rev A. 2026;113(4):042454. [DOI]
36. Lucamarini M, Yuan ZL, Dynes JF, Shields AJ. Overcoming the rate–distance limit of quantum key distribution without quantum repeaters. Nature. 2018;557(7705):400-403. [DOI]
37. Wang S, Yin ZQ, He DY, Chen W, Wang RQ, Ye P, et al. Twin-field quantum key distribution over 830-km fibre. Nat Photonics. 2022;16(2):154-161. [DOI]
38. Liu Y, Zhang WJ, Jiang C, Chen JP, Zhang C, Pan WX, et al. Experimental twin-field quantum key distribution over 1000 km fiber distance. Phys Rev Lett. 2023;130(21):210801. [DOI][PubMed]
39. Grosshans F, Grangier P. Continuous variable quantum cryptography using coherent states. Phys Rev Lett. 2002;88(5):057902. [DOI] [PubMed]
40. Grosshans F, Van Assche G, Wenger J, Brouri R, Cerf NJ, Grangier P. Quantum key distribution using Gaussian-modulated coherent states. Nature. 2003;421(6920):238-241. [DOI]
41. Hajomer AAE, Bruynsteen C, Derkach I, Jain N, Bomhals A, Bastiaens S, et al. Continuous-variable quantum key distribution at 10 GBaud using an integrated photonic-electronic receiver. Optica. 2024;11(9):1197. [DOI]
42. Zhang Y, Chen Z, Pirandola S, Wang X, Zhou C, Chu B, et al. Long-distance continuous-variable quantum key distribution over 202.81 km of fiber. Phys Rev Lett. 2020;125(1):010502. [DOI][PubMed]
43. Shao Y, Wang H, Pi Y, Huang W, Li Y, Liu J, et al. Phase noise model for continuous-variable quantum key distribution using a local local oscillator. Phys Rev A. 2019;104(3):032305. [DOI]
44. Wang XY, Guo XB, Jia YX, Zhang Y, Lu ZG, Liu JQ, et al. Accurate shot-noise-limited calibration of a time-domain balanced homodyne detector for continuous-variable quantum key distribution. J Light Technol. 2023;41(17):5518-5528. [DOI]
45. Matsuura T, Maeda K, Sasaki T, Koashi M. Finite-size security of continuous-variable quantum key distribution with digital signal processing. Nat Commun. 2021;12(1):252. [DOI][PubMed][PMC]
46. Kanitschar F, George I, Lin J, Upadhyaya T, Lütkenhaus N. Finite-size security for discrete-modulated continuous-variable quantum key distribution protocols. PRX Quantum. 2023;4(4):040306. [DOI]
47. Lupo C, Ouyang Y. Quantum key distribution with nonideal heterodyne detection: Composable security of discrete-modulation continuous-variable protocols. PRX Quantum. 2022;3:010341. [DOI]
48. Primaatmaja IW, Goh KT, Tan EY, Khoo JT, Ghorai S, Lim CC. Security of device-independent quantum key distribution protocols: A review. Quantum. 2023;7:932. [DOI]
49. Elshaari AW, Pernice W, Srinivasan K, Benson O, Zwiller V. Hybrid integrated quantum photonic circuits. Nat Photonics. 2020;14(5):285-298. [DOI]

50. Luo W, Cao L, Shi Y, Wan L, Zhang H, Li S, et al. Recent progress in quantum photonic chips for quantum communication and internet. Light Sci Appl. 2023;12(1):175. [DOI][PubMed][PMC]
51. Wang C, Zhang M, Chen X, Bertrand M, Shams-Ansari A, Chandrasekhar S, et al. Integrated lithium niobate electro-optic modulators operating at CMOS-compatible voltages. Nature. 2018;562(7725):101-104. [DOI]
52. 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(9A):L1217. [DOI]
53. 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(12):1953-1970. [DOI]
54. Reed GT, Mashanovich G, Gardes FY, Thomson DJ. Silicon optical modulators. Nat Photonics. 2010;4(8):518-526. [DOI]
55. Silverstone JW, Bonneau D, O'Brien JL, Thompson MG. Silicon quantum photonics. IEEE J Select Topics Quantum Electron. 2016;22(6):390-402. [DOI]
56. Paraïso TK, Roger T, Marangon DG, De Marco I, Sanzaro M, Woodward RI, et al. A photonic integrated quantum secure communication system. Nat Photonics. 2021;15(11):850-856. [DOI]
57. Zhu CX, Chen ZY, Li Y, Wang XZ, Wang CZ, Zhu YL, et al. Experimental quantum key distribution with integrated silicon photonics and electronics. Phys Rev Appl. 2022;17(6):064034. [DOI]
58. Zhen Z, Jin SY, Jie R, Xu XS. Integrated silicon photonics chip fabricated by CMOS compatible technology for low-bit-error-rate quantum key distribution. J Opt. 2023;25(11):115701. [DOI]
59. Kong L, Li Z, Li C, Cao L, Xing Z, Cao J, et al. Photonic integrated quantum key distribution receiver for multiple users. Opt Express. 2020;28(12):18449-18455. [DOI][PubMed]
60. Blumenthal DJ, Heideman R, Geuzebroek D, Leinse A, Roeloffzen C. Silicon nitride in silicon photonics. Proc IEEE. 2018;106(12):2209-2231. [DOI]
61. Roeloffzen CGH, Hoekman M, Klein EJ, Wevers LS, Timens RB, Marchenko D, et al. Low-loss Si_3N_4 TriPleX optical waveguides: Technology and applications overview. IEEE J Sel Top Quantum Electron. 2018;24(4):4400321. [DOI]
62. Zhang X, Bell BA, Mahendra A, Xiong C, Leong PHW, Eggleton BJ. Integrated silicon nitride time-bin entanglement circuits. Opt Lett. 2018;43(15):3469-3472. [DOI]
63. Fan YR, Lyu C, Yuan CZ, Deng GW, Zhou ZY, Geng Y, et al. Multi-wavelength quantum light sources on silicon nitride micro-ring chip. Laser Photonics Rev. 2023;17(10):2300172. [DOI]
64. Imany P, Jaramillo-Villegas JA, Odele OD, Han K, Leaird DE, Lukens JM, et al. 50-GHz-spaced comb of high-dimensional frequency-Bin entangled photons from an on-chip silicon nitride microresonator. Opt Express. 2018;26(2):1825-1840. [DOI][PubMed]
65. He M, Xu M, Ren Y, Jian J, Ruan Z, Xu Y, et al. High-performance hybrid silicon and lithium niobate Mach–Zehnder modulators for 100 Gbit s−1 and beyond. Nat Photonics. 2019;13(5):359-364. [DOI]
66. Smit M, Leijtens X, Ambrosius H, Bente E, van der Tol J, Smalbrugge B, et al. An introduction to InP-based generic integration technology. Semicond Sci Technol. 2014;29(8):083001. [DOI]
67. Liang D, Roelkens G, Baets R, Bowers JE. Hybrid integrated platforms for silicon photonics. Materials. 2010;3(3):1782-1802. [DOI]
68. Roelkens G, Liu L, Liang D, Jones R, Fang A, Koch B, et al. III-V/silicon photonics for on-chip and intra-chip optical interconnects. Laser Photonics Rev. 2010;4(6):751-779. [DOI]
69. Fathpour S. Emerging heterogeneous integrated photonic platforms on silicon. Nanophotonics. 2014;4(2):143-164. [DOI]
70. Paraïso TK, De Marco I, Roger T, Marangon DG, Dynes JF, Lucamarini M, et al. A modulator-free quantum key distribution transmitter chip. npj Quantum Inf. 2019;5:42. [DOI]
71. Ma C, Sacher WD, Tang Z, Mikkelsen JC, Yang Y, Xu F, et al. Silicon photonic transmitter for polarization-encoded quantum key distribution. Optica. 2016;3(11):1274. [DOI]
72. Cai H, Long CM, DeRose CT, Boynton N, Urayama J, Camacho R, et al. Silicon photonic transceiver circuit for high-speed polarization-based discrete variable quantum key distribution. Opt Express. 2017;25(11):12282-12294. [DOI][PubMed]
73. Hadfield RH. Single-photon detectors for optical quantum information applications. Nat Photonics. 2009;3(12):696-705. [DOI]
74. Zhang J, Itzler MA, Zbinden H, Pan JW. Advances in InGaAs/InP single-photon detector systems for quantum communication. Light Sci Appl. 2015;4(5):e286. [DOI]
75. Natarajan CM, Tanner MG, Hadfield RH. Superconducting nanowire single-photon detectors: Physics and applications. Supercond Sci Technol. 2012;25(6):063001. [DOI]
76. Beutel F, Gehring H, Wolff MA, Schuck C, Pernice W. Detector-integrated on-chip QKD receiver for GHz clock rates. npj Quantum Inf. 2021;7:40. [DOI]
77. Pernice WHP, Schuck C, Minaeva O, Li M, Goltsman GN, Sergienko AV, et al. High-speed and high-efficiency travelling wave single-photon detectors embedded in nanophotonic circuits. Nat Commun. 2012;3:1325. [DOI][PubMed][PMC]
78. Zheng X, Zhang P, Ge R, Lu L, He G, Chen Q, et al. Heterogeneously integrated, superconducting silicon-photonic platform for measurement-device-independent quantum key distribution. Adv Photon. 2021;3(5):1-8. [DOI]
79. Bruynsteen C, Vanhoecke M, Bauwelinck J, Xin Y. Integrated balanced homodyne photonic–electronic detector for beyond 20 GHz shot-noise-limited measurements. Optica. 2021;8(9):1146. [DOI]
80. Tasker JF, Frazer J, Ferranti G, Allen EJ, Brunel LF, Tanzilli S, et al. Silicon photonics interfaced with integrated electronics for 9 GHz measurement of squeezed light. Nat Photonics. 2021;15(1):11-15. [DOI]

81. Raffaelli F, Ferranti G, Mahler DH, Sibson P, Kennard JE, Santamato A, et al. A homodyne detector integrated onto a photonic chip for measuring quantum states and generating random numbers. Quantum Sci Technol. 2018;3(2):025003. [DOI]
82. Huang D, Fang J, Wang C, Huang P, Zeng GH. A 300-MHz bandwidth balanced homodyne detector for continuous variable quantum key distribution. Chin Phys Lett. 2013;30(11):114209. [DOI]
83. Jia Y, Wang X, Hu X, Hua X, Zhang Y, Guo X, et al. Silicon photonics-integrated time-domain balanced homodyne detector for quantum tomography and quantum key distribution. New J Phys. 2023;25(10):103030. [DOI]
84. Ding Y, Bacco D, Dalgaard K, Cai X, Zhou X, Rottwitt K, et al. High-dimensional quantum key distribution based on multicore fiber using silicon photonic integrated circuits. npj Quantum Inf. 2017;3:25. [DOI]
85. Zahidy M, Liu Y, Cozzolino D, Ding Y, Morioka T, Oxenløwe LK, et al. Photonic integrated chip enabling orbital angular momentum multiplexing for quantum communication. Nanophotonics. 2021;11(4):821-827. [DOI][PubMed][PMC]
86. Wen W, Chen Z, Lu L, Yan W, Xue W, Zhang P, et al. Realizing an entanglement-based multiuser quantum network with integrated photonics. Phys Rev Appl. 2022;18(2):024059. [DOI]
87. Sax R, Boaron A, Boso G, Atzeni S, Crespi A, Grünenfelder F, et al. High-speed integrated QKD system. Photon Res. 2023;11(6):1007. [DOI]
88. Jain N, Wittmann C, Lydersen L, Wiechers C, Elser D, Marquardt C, et al. Device calibration impacts security of quantum key distribution. Phys Rev Lett. 2011;107(11):110501. [DOI][PubMed]
89. Fung CF, Qi B, Tamaki K, Lo HK. Phase-remapping attack in practical quantum-key-distribution systems. Phys Rev A. 2007;75(3):032314. [DOI]
90. Xu F, Qi B, Lo HK. Experimental demonstration of phase-remapping attack in a practical quantum key distribution system. New J Phys. 2010;12(11):113026. [DOI]
91. Harris NC, Ma Y, Mower J, Baehr-Jones T, Englund D, Hochberg M, et al. Efficient, compact and low loss thermo-optic phase shifter in silicon. Opt Express. 2014;22(9):10487-10493. [DOI][PubMed]
92. Wang X, Jia Y, Guo X, Liu J, Wang S, Liu W, et al. Silicon photonics integrated dynamic polarization controller. Chin Opt Lett. 2022;20(4):041301. Available form: https://opg.optica.org/col/abstract.cfm?URI=col-20-4-041301
93. Zhang GW, Chen W, Fan-Yuan GJ, Zhang L, Wang FX, Wang S, et al. Polarization-insensitive quantum key distribution using planar lightwave circuit chips. Sci China Inf Sci. 2022;65(10):200506. [DOI]
94. Ma HX, Huang P, Wang T, Bai DY, Wang SY, Bao WS, et al. Security bound of continuous-variable measurement-device-independent quantum key distribution with imperfect phase reference calibration. Phys Rev A. 2019;100(5):052330. [DOI]
95. Yuan ZL, Fröhlich B, Lucamarini M, Roberts GL, Dynes JF, Shields AJ. Directly phase-modulated light source. Phys Rev X. 2016;6(3):031044. [DOI]
96. Liu H, Wang J, Ma H, Sun S. Polarization-multiplexing-based measurement-device-independent quantum key distribution without phase reference calibration. Optica. 2018;5(8):902. [DOI]
97. Wang C, Song XT, Yin ZQ, Wang S, Chen W, Zhang CM, et al. Phase-reference-free experiment of measurement-device-independent quantum key distribution. Phys Rev Lett. 2015;115(16):160502. [DOI][PubMed]
98. Marie A, Alléaume R. Self-coherent phase reference sharing for continuous-variable quantum key distribution. Phys Rev A. 2017;95:012316. [DOI]
99. Alaghbari KA, Rumyantsev K, Eltaif T, Elmabrok O, Lim HS. Adaptive modulation for continuous-variable quantum key distribution with real local oscillators under phase attack. IEEE Photonics J. 2021;13(5):7600107. [DOI]
100. Pereira D, Almeida M, Facão M, Pinto AN, Silva NA. Impact of receiver imbalances on the security of continuous variables quantum key distribution. EPJ Quantum Technol. 2021;8(1):22. [DOI]
101. Lin J, Lütkenhaus N. Trusted detector noise analysis for discrete modulation schemes of continuous-variable quantum key distribution. Phys Rev Appl. 2020;14(6):064030. [DOI]
102. 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(3):032611. [DOI]
103. Tamaki K, Curty M, Kato G, Lo HK, Azuma K. Loss-tolerant quantum cryptography with imperfect sources. Phys Rev A. 2014;90(5):052314. [DOI]
104. Yin HL, Zhou MG, Gu J, Xie YM, Lu YS, Chen ZB. Tight security bounds for decoy-state quantum key distribution. Sci Rep. 2020;10(1):14312. [DOI][PubMed][PMC]
105. Karinou F, Brunner HH, Fung CF, Comandar LC, Bettelli S, Hillerkuss D, et al. Toward the integration of CV quantum key distribution in deployed optical networks. IEEE Photonics Technol Lett. 2018;30(7):650-653. [DOI]
106. Kumar R, Qin H, Alléaume R. Coexistence of continuous variable QKD with intense DWDM classical channels. New J Phys. 2015;17(4):043027. [DOI]
107. Chu B, Zhang Y, Zhao Y, Xu Y, Chen X, Wang X, et al. Crosstalk-induced impact of coexisting DWDM network on continuous-variable QKD. In: 2020 16th international conference on the design of reliable communication networks DRCN 2020; 2020 Mar 25-27; Milan, Italy. Piscataway: IEEE; 2020. p. 1-5. [DOI]
108. Huang Y, Zhang Y, Shen T, Huang G, Yu S. Experimental demonstration of upstream continuous-variable QKD access network. In: 2020 conference on lasers and electro-optics (CLEO); 2020 May 10-15; San Jose, USA. Piscataway: IEEE; 2020. p. 1-2. [DOI]
109. Xie J, Zhang L, Wang Y, Huang D. Deep neural network based reconciliation for CV-QKD. Photonics. 2022;9(2):110. [DOI]

110. Avesani M, Calderaro L, Schiavon M, Stanco A, Agnesi C, Santamato A, et al. Full daylight quantum-key-distribution at 1550 nm enabled by integrated silicon photonics. npj Quantum Inf. 2021;7:93. [DOI]
111. Luo W, Cao L, Cai H, Karim MF, Kwek LC, Liu AQ. A silicon photonic chip-based system for 2.5-GHz quantum key distribution (QKD). In: 2024 optical fiber communications conference and exhibition (OFC); 2024 Mar 24-28; San Diego, USA. Piscataway: IEEE; 2024. p. 1-3. [DOI]
112. Cao L, Luo W, Wang YX, Zou J, Yan RD, Cai H, et al. Chip-based measurement-device-independent quantum key distribution using integrated silicon photonic systems. Phys Rev Appl. 2020;14:011001. [DOI]
113. Li L, Wang T, Li X, Huang P, Guo Y, Lu L, et al. Continuous-variable quantum key distribution with on-chip light sources. Photon Res. 2023;11(4):504. [DOI]
114. Piétri Y, Vidarte LT, Schiavon M, Grangier P, Rhouni A, Diamanti E. CV-QKD receiver platform based on a silicon photonic integrated circuit. In: 2023 Optical Fiber Communications Conference and Exhibition (OFC); 2023 Mar 5-9; San Diego, USA. Piscataway: IEEE; 2023. p. 1-3. [DOI]
115. Zhu J, Zhou X, Ding H, Liu J, Zhang C, Li J, et al. One-decoy-state quantum key distribution with advantage distillation based on planar-lightwave-circuit-integration modules. Phys Rev A. 2025;111:012608. [DOI]
116. Liu S, Jia Y, Shi Y, Hou Y, Wang P, Zhang Y, et al. Continuous-variable quantum key distribution over 50.4 km fiber using an integrated silicon photonic transmitter and receiver. Photon Res. 2025;13(11):3141. [DOI]
117. Cao L, Li S, Yu H, Chin LK, Wang X, Zhang X, et al. Quantum photonic chip for practical high-rate continuous-variable quantum key distribution. Photon Res. 2026;14(6):2382. [DOI]
118. Wei K, Hu X, Du Y, Hua X, Zhao Z, Chen Y, et al. Resource-efficient quantum key distribution with integrated silicon photonics. Photon Res. 2023;11(8):1364. [DOI]
119. Du Y, Li BH, Hua X, Cao XY, Zhao Z, Xie F, et al. Chip-integrated quantum signature network over 200 km. Light Sci Appl. 2025;14(1):108. [DOI][PubMed][PMC]
120. Li W, Zhang L, Tan H, Lu Y, Liao SK, Huang J, et al. High-rate quantum key distribution exceeding 110 Mb s–1. Nat Photonics. 2023;17(5):416-421. [DOI]
121. Boaron A, Boso G, Rusca D, Vulliez C, Autebert C, Caloz M, et al. Secure quantum key distribution over 421 km of optical fiber. Phys Rev Lett. 2018;121(19):190502. [DOI][PubMed]
122. Grünenfelder F, Boaron A, Resta GV, Perrenoud M, Rusca D, Barreiro C, et al. Fast single-photon detectors and real-time key distillation enable high secret-key-rate quantum key distribution systems. Nat Photonics. 2023;17(5):422-426. [DOI][PubMed][PMC]
123. Korzh B, Lim CCW, Houlmann R, Gisin N, Li MJ, Nolan D, et al. Provably secure and practical quantum key distribution over 307 km of optical fibre. Nat Photonics. 2015;9(3):163-168. [DOI]
124. Yan W, Zheng X, Wen W, Lu L, Du Y, Lu YQ, et al. A measurement-device-independent quantum key distribution network using optical frequency comb. npj Quantum Inf. 2025;11:97. [DOI]
125. Zheng Y, Wang H, Jia X, Huang J, Yuan H, Zhai C, et al. Large-scale quantum communication networks with integrated photonics. Nature. 2026;651(8104):68-75. [DOI]
126. Wang FX, Zheng ST, Huang L, Zhang GW, Wang GS, Ding WJ, et al. Microcomb-driven large-scale fully connected quantum network. Nat Commun. 2026;17:9319. [DOI]
127. Zhang L, Pan J, Chen TY, Li ZP, Lu Y, Li W, et al. A photonic integrated long-distance quantum communication network. Nat Photonics. 2026;20(8):876-882. [DOI]
128. Jouguet P, Kunz-Jacques S, Diamanti E. Preventing calibration attacks on the local oscillator in continuous-variable quantum key distribution. Phys Rev A. 2013;87(6):062313. [DOI]
129. Lucamarini M, Choi I, Ward MB, Dynes JF, Yuan ZL, Shields AJ. Practical security bounds against the Trojan-horse attack in quantum key distribution. Phys Rev X. 2015;5(3):031030. [DOI]
130. Kang X, Ye P, Wang S, Zhang GW, Wang ZH, Chen JL, et al. Effect of femtosecond-pulse-injection silicon photonic modulators on the security of quantum key distribution. Phys Rev Appl. 2025;23(2):024014. [DOI]
131. Tsai CW, Yang CW, Lin J, Chang YC, Chang RS. Quantum key distribution networks: Challenges and future research issues in security. Appl Sci. 2021;11(9):3767. [DOI]
132. Lella E, Schmid G. On the security of quantum key distribution networks. Cryptography. 2023;7(4):53. [DOI]
133. Braun RP, Ritter M, Doering R, Geitz M. Berlin OpenQKD testbed evaluating quantum key distribution in provider networks. In: Proceedings of the 2023 8th International Conference on Systems, Control and Communications; 2023 Oct 20-22; Chongqing, China. New York: Association for Computing Machinery; 2024. p. 41-51. [DOI]
134. Zhong X, Wang W, Mandil R, Lo HK, Qian L. Simple multiuser twin-field quantum key distribution network. Phys Rev Appl. 2022;17:014025. [DOI]
135. Xu J, Ma X, Liu J, Zhang C, Li H, Zhou X, et al. Automatically identifying imperfections and attacks in practical quantum key distribution systems via machine learning. Sci China Inf Sci. 2024;67(10):202501. [DOI]
136. Ren ZA, Chen YP, Liu JY, Ding HJ, Wang Q. Implementation of machine learning in quantum key distributions. IEEE Commun Lett. 2021;25(3):940-944. [DOI]
137. Aldama J, Sarmiento S, López Grande IH, Signorini S, Vidarte LT, Pruneri V. Integrated QKD and QRNG photonic technologies. J Light Technol. 2022;40(23):7498-7517. [DOI]

138. Li X, Wang LL, Zhang JS, Chen W, Wang Y, Wu D, et al. Quantum key distribution transmitter chip based on hybrid-integration of silica and lithium niobates. Chin Phys B. 2022;31(6):064212. [DOI]
139. 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. [DOI]
140. 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. 2022;40(7):2052-2059. [DOI]
141. Chen JP, Zhang C, Liu Y, Jiang C, Zhang WJ, Han ZY, et al. Twin-field quantum key distribution over a 511 km optical fibre linking two distant metropolitan areas. Nat Photonics. 2021;15(8):570-575. [DOI]
142. Bäuml S, Pascual-García C, Wright V, Fawzi O, Acín A. Security of discrete-modulated continuous-variable quantum key distribution. Quantum. 2024;8:1418. [DOI]
143. Wang P, Wang X, Li Y. Continuous-variable measurement-device-independent quantum key distribution with source-intensity errors. Phys Rev A. 2020;102(2):022609. [DOI]
144. Shao Y, Li Y, Wang H, Pan Y, Pi Y, Zhang Y, et al. Phase-reference-intensity attack on continuous-variable quantum key distribution with a local local oscillator. Phys Rev A. 2022;105(3):032601. [DOI]
145. Huang L, Zhang Y, Yu S. Continuous-variable measurement-device-independent quantum key distribution with one-time shot-noise unit calibration. Chin Phys Lett. 2021;38(4):040301. [DOI]
146. Pirandola S. Composable security for continuous variable quantum key distribution: Trust levels and practical key rates in wired and wireless networks. Phys Rev Research. 2021;3(4):043014. [DOI]
147. Wang S, Huang P, Liu M, Wang T, Wang P, Zeng G. Phase compensation for free-space continuous-variable quantum key distribution. Opt Express. 2020;28(8):10737-10745. [DOI][PubMed]
148. Ghalaii M, Pirandola S. Continuous-variable measurement-device-independent quantum key distribution in free-space channels. Phys Rev A. 2023;108(4):042621. [DOI]
149. Bai B, Huang J, Qiao GR, Nie YQ, Tang W, Chu T, et al. 18.8 Gbps real-time quantum random number generator with a photonic integrated chip. Appl Phys Lett. 2021;118(26):264001. [DOI]
150. Wang H, Pi Y, Huang W, Li Y, Shao Y, Yang J, et al. High-speed Gaussian-modulated continuous-variable quantum key distribution with a local local oscillator based on pilot-tone-assisted phase compensation. Opt Express. 2020;28(22):32882-32893. [DOI][PubMed]
151. Xing Z, Li X, Ruan X, Luo Y, Zhang H. Phase compensation for continuous variable quantum key distribution based on convolutional neural network. Photonics. 2022;9(7):463. [DOI]
152. Kanitschar F, Pacher C. Optimizing continuous-variable quantum key distribution with phase-shift keying modulation and postselection. Phys Rev Appl. 2022;18(3):034073. [DOI]
153. Liu WB, Li CL, Xie YM, Weng CX, Gu J, Cao XY, et al. Homodyne detection quadrature phase shift keying continuous-variable quantum key distribution with high excess noise tolerance. PRX Quantum. 2021;2(4):040334. [DOI]
154. Huang Y, Zhang Y, Xu B, Huang L, Yu S. A modified practical homodyne detector model for continuous-variable quantum key distribution: Detailed security analysis and improvement by the phase-sensitive amplifier. J Phys B At Mol Opt Phys. 2020;54(1):015503. [DOI]

Publisher's Note

Science Exploration remains a neutral stance on jurisdictional claims in published maps and institutional affiliations. The views expressed in this article are solely those of the author(s) and do not reflect the opinions of the Editors or the publisher.