# An All-Silicon Approach to Large-Scale Quantum Key Distribution

Valeria Saggio, Florian Honz, Hannes Hübel and Bernhard Schrenk

*Center for Digital Safety and Security, AIT Austrian Institute of Technology, Giefinggasse 4, 1210 Vienna, Austria*

*valeria.saggio@ait.ac.at*

**Abstract**

We discuss an all-silicon approach that enables miniaturization of Quantum Key Distribution (QKD) components and targets cost effectiveness. This facilitates the widespread adoption of QKD in standard communication infrastructures, opening the door to new application domains currently out of reach with conventional QKD technologies.

## Introduction

Technological advances in the field of quantum computing are anticipated to pose significant risks to classical communication systems by potentially exposing them to security breaches. This threat is effectively addressed by the introduction of quantum key distribution (QKD), a protocol harnessing the laws of quantum physics to enable information-theoretic secure (ITS) encryption and thus render communication networks intrinsically resilient to security risks [1]. Despite its transformative potential across a wide array of sectors where confidentiality and secure data exchange are paramount – ranging from e.g. finance and banking to the healthcare domain and telecommunications [2] – QKD's practical deployment for mass-scale applications faces several key technological and economic challenges [3]. In particular, the integration of QKD components into existing information & communication technology (ICT) infrastructures requires the development of a QKD solution targeting both ultra compact component footprints and cost-effective production cycles. In the following, we will discuss recent progress towards this goal, highlighting advancements in QKD devices that are compatible with future large-scale deployment. These developments open the door to the widespread adoption of QKD into communication domains such as secure intra-datacenter links or personal wireless and mobile platforms, which have so far remained unexplored due to limitations in size, costs, and overall complexity of current QKD technologies.

## An All-Silicon Approach for Quantum Key Distribution

Our proposed scheme to render QKD broadly accessible and deployable at scale leverages the maturity of the silicon microelectronic and photonic industry to *(i)* overcome key barriers to chip-scale QKD development, enabling component miniaturization and seamless photonic and electronic co-integration, and *(ii)* effectively constrain the production and assembly costs through the employment of streamlined fabrication techniques. To enable full compatibility of QKD applications with the integration standards of modern microelectronics in e.g. ICT networks or consumer electronics, chip-scale QKD components become a necessity. While the migration from bulk devices towards miniaturization and integration of QKD components into photonic integrated circuits (PICs) has already proven its advantages for QKD applications as well as quantum random number generation [4-5], present-day PIC solutions rely on the use of III-V semiconductors to enable light generation in QKD transmitters. This implies hermetic packaging and a notable increased complexity in the fabrication process compared to traditional silicon-based technologies, hampering the commercial viability of III-V-based QKD devices. Additionally, the elevated costs for co-assembly pose yet another barrier that impedes their widespread adoption in mass-market QKD deployments. It seems therefore natural to migrate towards an all-silicon approach, which is set to exploit the potential of the monolithic silicon industry to enable compactness of QKD modules, seamless microelectronics co-integration, and lower production costs [6].

Silicon is however characterized by an indirect bandgap, which poses a fundamental limitation to its use as an efficient light emitter in conventional photonic applications requiring on-chip optical sources. Our approach proposes the use of engineered SiGe photonic waveguide platforms, designed to exploit quasi-direct bandgap behavior and thus emit light with sufficiently strong optical power for transmission of quantum states in QKD applications [6]. The intrinsic incoherent nature of the emitted light makes this source effectively compatible with polarization-encoded QKD implementations, allowing secure quantum key exchange without the need for phase coherence or phase stabilization.

Recent results [7-8] show the viability of this approach, presenting the first demonstrations of monolithic silicon-based QKD components, and in particular proving that silicon-based light sources are capable of meeting the operational requirements of QKD implementations and vastly simplifying the design and assembly of QKD transmitters. It has been shown [7] that a monolithic silicon chip solution for a QKD transmitter can be employed in a BB84 discrete-variable (DV) QKD protocol. The transmitter includes a 90-$\mu$m long forward-biased lateral SiGe PIN junction to serve as light source in the telecom C-band, coupled to a 1D grating coupler on a silicon-on-insulator platform for coupling at the rear facet of the light source, and 2D grating couplers for outcoupling into the QKD transmission channels. The transmitter further comprises a state preparation circuit for the implementation of polarization-encoded BB84 protocol. Signal states are generated at a rate of 100 MHz with one out of four possible polarizations. The generated states are used to implement a BB84 DV QKD protocol over a 45.9 km-long fiber link to achieve a secure key rate of 655 b/s at a quantum bit error rate (QBER) of 5.05%. This approach opens new possibilities for fully integrated, CMOS-compatible quantum communication systems on a silicon chip, and would be particularly well-suited for networks with a centralized receiver, where the overall system complexity can be concentrated at a single node, enabling the use of highly simplified and low-cost silicon-based QKD transmitters at the network edge.

The drastic simplification of QKD hardware through the proposed all-silicon approach is a significant first step toward the adoption of QKD in several ICT infrastructure-heavy domains such as intra-facility links, metro, or enterprise networks. However, one further step can be taken to adopt QKD in optical wireless communication (OWC), and in particular free-space optical links (FSO) scenarios, which are key to QKD implementations in e.g. personal mobile devices. Recent results [9,10] show a novel alignment-tolerant optical hotspot technology, which can enable low-loss coupling in a fiber-wireless-fiber scenario. This approach is based on the adoption of a fiber-based focal plane array beam former acting as an air interface between two single-mode optical fiber ports for the establishment of an FSO link. This technology can unlock novel QKD applications in that it could enable free-space optical key exchange between mobile QKD transmitters and an optical access point.

## Conclusion

We have illustrated the potential of an all-silicon approach for QKD, discussing recent results on the suitability of silicon-based light sources for quantum-safe communication and highlighting the advantages of silicon photonics for CMOS-compatible fabrication techniques that enable ultra-small form factors and eliminate the need for complex heterogeneous integration, thus bringing down the manufacturing costs. Moreover, we have discussed how novel QKD application domains could be accessed with our proposed technology. These may include intra-facility secure networks and handheld personal devices requiring wireless coupling between the mobile QKD transmitter and an optical hotspot. Our results highlight a promising path toward a widespread adoption of QKD in diverse communication infrastructures, many of which are currently out of reach with present-day QKD technologies.


## Acknowledgments

The work was supported by the European Innovation Council under the Horizon Europe program under grant agreement no. 101187539, and through the QuantERA II Programme (GA No 101017733) and the Austrian FFG (GA No FO999906040).


## References


[1] D. Rusca, and N. Gisin, "Quantum cryptography: An overview of quantum key distribution", *arXiv preprint arXiv:2411.04044* (2024).

[2] S. Cobourne, "Quantum key distribution protocols and applications", *Surrey TW20 0EX*, 2011, England.

[3] E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, "Practical challenges in quantum key distribution*", npj Quantum Information*, 2(1), 1-12 (2016).

[4] A. Trenti, et al., "On-chip quantum communication devices", *Journal of Lightwave Technology*, 40(23), 7485-7497, 2022.

[5] T. K. Paraïso, et al., "A photonic integrated quantum secure communication system", *Nature Photonics* 15, 850–856 (2021).

[6] B. Schrenk, "Making Quantum Key Distribution a Commodity: The All-Silicon Approach", *In 2024 IEEE 10th International Conference on Photonics (ICP)* (pp. 20-22), 2024, IEEE.

[7] F. Honz, et al., "World's First Monolithic SiGe QKD Transmitter Chip", *in Proc. Optical Fiber Communication Conf. (OFC), San Francisco, United States*, 2025, paper Th4D.7.

[8] F. Honz, et al., "Towards an All-Silicon QKD Transmitter Sourced by a Ge-on-Si Light Emitter", *IEEE Journal of Selected Topics in Quantum Electronics*, 30 (1: Single-Photon Technologies and Applications), 1-9, 2023.

[9] F. Honz, and B. Schrenk, "Alignment-Tolerant Optical Fi-Wi-Fi Bridge Assisted by a Focal Plane Array Beamformer as Air Interface", *Journal of Lightwave Technology*, vol. 43, no. 13, pp. 6187-6193, 2025.

[10] F. Honz, et al., "FPA Beamforming for Alignment-Tolerant FSO QKD Links", in *Optical Fiber Communication Conference (OFC) 2025*, Technical Digest Series (Optica Publishing Group, 2025), paper Th3I.3.