Overview on Hardware Adaptation for Continuous-Variable Quantum Key Distribution Systems: Opportunities with RISC-V Architectures

Glenda Barbosa do Nascimento[*,1], **Linton Thiago Costa Esteves**[1], **Wagner Luiz Alves de Oliveira**[2], **Nelson Alves Ferreira Neto**[1]

[1]*QuIIN - Quantum Industrial Innovation, EMBRAPII CIMATEC Competence Center in Quantum Technologies, SENAI CIMATEC, Salvador, BA, Brazil.*

[1]*Federal University of Recôncavo da Bahia, Center for Exact and Technological Sciences, Cruz das Almas, Bahia, Brazil*

[2]*Graduate Program in Electrical and Computer Engineering, Federal University of Bahia, 40210-630, Salvador, Brazil*

[*]*Corresponding author: glenda.nascimento@fbter.org.br*

Abstract: Continuous-variable quantum key distribution (CV-QKD) enables secure key exchange by exploiting the quantum properties of optical field quadratures. While CV-QKD protocols offer strong potential due to their compatibility with existing optical infrastructure, their practical deployment is limited by the high computational complexity of digital signal processing (DSP) and post-processing tasks. Operations such as low-density parity-check (LDPC) decoding for information reconciliation (IR), privacy amplification (PA), carrier recovery (CR), phase recovery (PR), and statistical estimation must be performed under stringent real-time, energy, and security constraints. Conventional programmable hardware platforms comprising general-purpose central processing units (CPUs) and graphics processing units (GPUs) often lack the efficiency required for secure and efficient CV-QKD processing in embedded or resource-constrained environments. In contrast, hard-coded application-specific integrated circuit (ASIC) solution do not provide the flexibility demanded by evolving protocols. This paper do a overview on hardware adaptation strategy based on the open fifth-generation Reduced Instruction Set Computing (RISC-V). By leveraging its modularity and extensibility, we explore the design of custom instruction sets and dedicated co-processors is explored to accelerate critical CV-QKD operations. This includes architecture-level enhancements for DSP and post-processing modules, such as CR, PR, IR, PA, and parameter estimation. The proposed approach facilitates co-design between evolving QKD protocols and hardware implementations, enabling transparent, efficient, and scalable solutions. The RISC-V-based methodology addresses CV-QKD challenges through specialized instruction extensions for dedicated processing and custom co-processors for real-time operations. Furthermore, RISC-V can enhance energy efficiency via dynamic voltage scaling and low-power modes, while its open-source nature ensures cryptographic transparency and security verification. Ultimately, this work establishes a foundation for energy-efficient and quantum-secure processor architectures capable of meeting CV-QKD demands and advancing cryptographic hardware.

Keywords: Quantum key distribution, Hardware acceleration, RISC-V architecture, Post-processing, Secure communication.

1. Introduction

Designing secure, efficient, and reconfigurable next-generation cryptographic systems hardware has become a critical task [1]. In this context, open and modular architectures such as the RISC-V offer a unique opportunity to rethink how computing platforms are tailored to quantum communication protocols, enabling hardware/software co-design that aligns with both flexibility and long-term trust [2].

This discussion becomes even more relevant when applied to CV-QKD systems [3]. While CV-QKD protocols offer significant advantages, such as compatibility with existing optical infrastructures and higher key generation rates, they impose substantial computational demands during the post-processing phase. Tasks like LDPC [4] used into IR, parameter estimation [5], and Toeplitz hash for PA require high throughput, numerical precision, and efficient memory usage, often in real-time or embedded environments [6]. Traditional

programmable platforms, such as general-purpose CPUs [7], DSPs [8], and GPUs [9], face limitations in terms of energy consumption and scalability. In contrast, hard-coded ASICs do not provide flexibility for long-term protocol adaptation. This exposes a clear gap: developing secure quantum protocols is not sufficient on its own, as the supporting hardware must also be adapted accordingly [10].

In light of this challenge, this work proposes a theoretical approach for hardware adaptation using the RISC-V architecture to support CV-QKD systems. The central research question is: how can RISC-V be tailored to meet the specific computational requirements of quantum key distribution based on continuous variables, while ensuring energy efficiency, hardware-level security, and architectural flexibility? The hypothesis is that through custom instruction extensions, dedicated functional units, and secure hardware mechanisms, it is possible to design computing platforms optimized for CV-QKD DSP and post-processing tasks such as IR, PA, CR, PR, and parameter estimation, all within an auditable and customizable framework [11]. The objective of this article is to explore a conceptual overview of how RISC-V can serve as an option for hardware platforms specialized in quantum cryptographic applications, with a focus on CV-QKD. By identifying the computational bottlenecks in the post-processing pipeline, and mapping them to architectural opportunities within the RISC-V ecosystem, this work outlines a direction for the development of open, efficient, and secure quantum hardware platforms, suitable for real-time operation and embedded deployment [1].

The structure of this paper is organized as follows: Section 2 presents the fundamental concepts of Continuous-Variable Quantum Key Distribution (CV-QKD) systems, emphasizing the post-processing algorithms and their associated computational challenges. Section 3 introduces the RISC-V philosophy, providing the necessary architectural background to understand its potential for domain-specific customization. Section 4 explores the opportunities of leveraging RISC-V architectures to address the identified performance, flexibility, and security gaps in CV-QKD implementations. Section 5 discusses the expected benefits, open challenges, and potential research directions. Finally, Section 6 concludes the paper by summarizing the contributions and reinforcing the role of hardware adaptation in advancing secure quantum communication

2. Fundamentals of CV-QKD Systems

CV-QKD protocols rely on the transmission of quantum states encoded in the conjugate quadratures of the electromagnetic field. These quadratures, denoted as $\hat{X}$ and $\hat{P}$ (representing the amplitude and phase quadrature operators), correspond to orthogonal components of the optical field. Un-

like discrete-variable QKD (DV-QKD), which encodes information in discrete degrees of freedom such as photon polarization or arrival time, CV-QKD leverages continuous quadrature measurements, enabling the use of standard telecommunications components like coherent detectors [11].

2.1. Transmission with Alice and Bob

A typical implementation of a CV-QKD system involves a transmitter (Alice) and a receiver (Bob), as shown in Figure 1. Alice prepares coherent states by modulating the amplitude and phase quadratures operators ($\hat{X}$ and $\hat{P}$) of a laser beam using Gaussian-distributed random numbers with electro-optic modulators. The modulated light is then sent through a quantum channel, which can be either an optical fiber or a Free-Space Optics (FSO) link [12].

Bob receives the optical signal and performs quadrature measurements using either: homodyne detection, randomly selecting to measure either X or P quadrature per measurement interval; or heterodyne detection, simultaneously measuring both quadratures. Both methods require a local oscillator phase-synchronized with Alice's laser. The measurement results are continuous values (not binary) that are later discretized during post-processing. This process is highly sensitive to channel loss and noise, meaning not all data is useful for key generation [3].

It is assumed that a potential eavesdropper (Eve) may intercept and resend the signal transmitted through the quantum channel. When performing quantum measurements, Eve introduces disturbances detectable as excess noise in Bob's measurements due to the quantum no-cloning theorem and uncertainty principle.

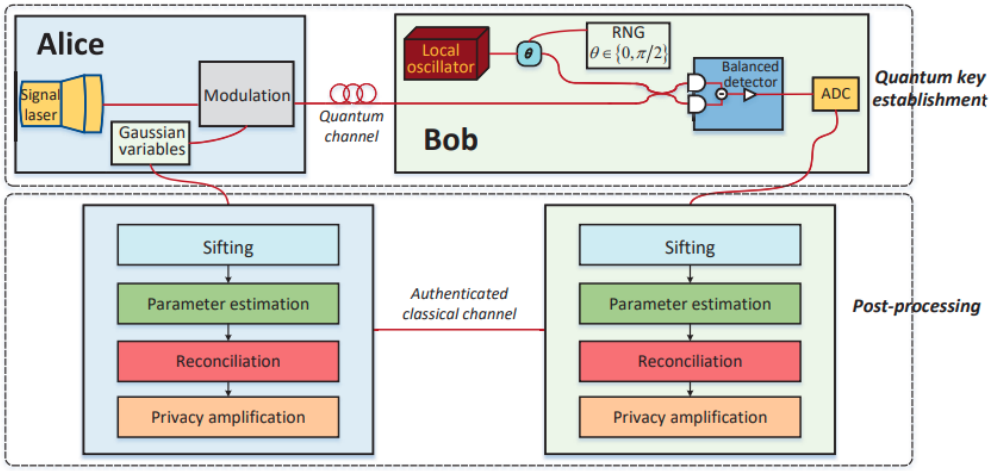
Using parameter estimation techniques, Alice and Bob analyze the transmittance (T) and excess noise (ξ) to quantify Eve's potential information and ensure key security [14].

2.2. Information Reconciliation

IR is a critical stage in CV-QKD systems, where the continuous-variable measurements from Alice and Bob are discretized into binary sequences using quantization techniques such as *slicing*. This process divides the continuous signal range into defined regions (bins), each assigned a bit value. However, due to channel noise and measurement imperfections, Alice's and Bob's sequences exhibit discrepancies [13].

Through classical communication technique, both parties perform reconciliation using error-correcting codes, most notably LDPC codes. While LDPC coding achieves near-capacity correction with minimal information leakage to eavesdroppers, it introduces significant computational burdens. High-performance LDPC decoding requires large block sizes ($> 10^6$ bits), parallel processing, and precision arithmetic (floating-point or fixed-point), particularly un-

Figure 1: Schematic diagram of the CV-QKD system [13].



der low signal-to-noise ratio (SNR) conditions. Implementing such algorithms efficiently on general-purpose CPUs is often impractical for real-time operation. Accelerators like GPUs can address throughput demands but face limitations in energy efficiency and flexibility for embedded or edge deployments [15].

2.3. Privacy Amplification

PA is the final post-processing step in CV-QKD systems. Its role is to reduce any residual information potentially acquired by an eavesdropper during transmission and reconciliation to a negligible level. This is achieved using cryptographic hash functions from the universal class, such as Toeplitz matrices, which compress a long, partially secure key to a shorter, information-theoretically secure key.

From a hardware perspective, PA presents significant computational challenges. Operations involve large matrix multiplications (e.g., Toeplitz-vector products) that can be optimized through fast Fourier transforms (FFT), requiring both high throughput (>10 Gbps) and bit-accurate precision [16].

3. The RISC-V Philosophy

RISC-V is an open standard instruction set architecture (ISA) based on Reduced Instruction Set Computing (RISC) principles. It prioritizes hardware efficiency through a minimal base instruction set of simple, frequently used operations [1]. This deliberate minimalism enables inherently simple, compact, and fast hardware for instruction decoding and pipeline implementation [2].

The architecture minimizes complexity by maintaining a small core instruction set, reducing silicon area, power consumption, and design verification overhead. While complex instructions in other ISAs may be used infrequently, they introduce pervasive control logic overhead that impacts even basic operations [2].

RISC-V's extensible modular design embodies this philosophy, organizing functionality into optional standard extensions. Far from limiting capability, this simplicity enables complex operations through optimized instruction sequences while avoiding unnecessary hardware complexity penalties. This combination of efficiency and customizability makes RISC-V particularly suitable for domain-specific systems like CV-QKD processors.

4. Opportunities with RISC-V Architectures

The evolution of CV-QKD systems demands adaptable and efficient hardware solutions capable of handling challenging post-processing tasks and stringent security requirements. In this context, RISC-V architectures stand out as a strategic opportunity, offering an open and flexible platform. Its core features align well with the implementation challenges of such systems [17].

4.1. Customization for QKD Post-Processing

One of RISC-V's most significant advantages lies in its modular and open-source architecture, which enables a high degree of customization. In the context of CV-QKD, this flexibility allows the development of processor cores specifically optimized for control and coordination tasks during the post-processing phase, without incurring the overhead typically associated with proprietary architectures. As shown in Figure 2, such processor cores can be designed with a lightweight and efficient microarchitectural structure, tailored precisely to the application's performance and resource constraints.

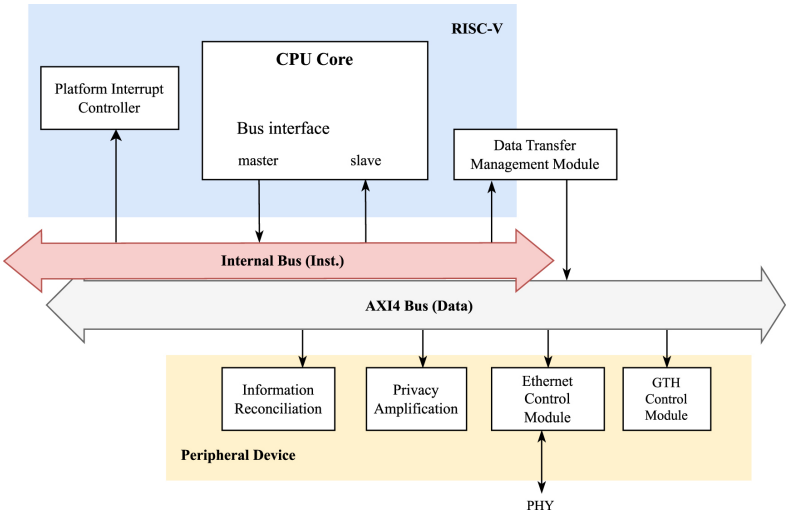
RISC-V also supports the integration of custom instruction set extensions (ISA extensions), such as those for 32-bit integer operations (RV32I) and partial support for multiplication and division (RV32M) [2]. This enables the RISC-V core to efficiently execute the arithmetic and logical operations required for post-processing, while maintaining a lightweight hardware structure. Furthermore, native support for interrupt handling mechanisms is another strong point, ensuring fast responses to external events or system requests [13].

4.2. Heterogeneous Architectures

The true potential of RISC-V architecture for CV-QKD lies in its ability to act as the central controller in heterogeneous architectures, where the most demanding computational tasks are offloaded to dedicated hardware accelerators [18]. This approach frees the RISC-V core to focus on control and decision-making operations, while specialized modules handle intensive processing. Examples of how this is applied include:

1. **Optimized Information Reconciliation:** Dedicated modules can be designed to process the LDPC parity-check matrix, using compact representations that drastically reduce storage requirements (as demonstrated by Xuan Wen et al [13], where reconciliation

Figure 2: RISCV CPU Interface [1].



protocols achieve near-optimal efficiencies, this approach can reduce storage by up to 99% for long codes). Modularity enables the implementation of LDPC decoders with parallel submodules and fixed-point arithmetic, optimizing throughput and resource usage, thus overcoming the typical complexity bottleneck of this stage.

2. **Accelerated Privacy Amplification:** Multiply-Accumulate (MAC) units specialized in Galois Fields GF(2) can be developed to speed up privacy amplification operations, efficiently transforming the reconciled key into a highly secure final key [16].

3. **Data Transfer Management (DTM):** RISC-V architecture greatly benefits from integration with data transfer management modules based on protocols such as AXI. These modules can act as independent bus masters, managing large volumes of data between peripherals without constant CPU intervention. This frees the RISC-V core for critical control tasks, improving responsiveness and overall system efficiency [1].

4.3. High-Performance Bus and Modularity

The adaptability of RISC-V facilitates the implementation of split-bus architectures, separating instruction and data traffic. This is crucial for CV-QKD systems, as it allows:

1. **Bandwidth Optimization:** Different bandwidth requirements for instructions and data can be handled independently, avoiding bottlenecks and contention.

2. **High-Speed Data Transmission:** As presented and discussed by Wu et al. [1], the use of high-performance data buses, such as AXI4-full (running at 200 MHz with 128-bit width), enables efficient bulk data transfer, essential for the throughput required in

QKD post-processing. This capability supports task-level pipelining for computational modules, ensuring continuous and uninterrupted data flow.

Adhering to a modular design philosophy is fundamental to the RISC-V paradigm. This means peripherals can be designed to be seamlessly integrated, with memory-mapped data buffers at module interfaces. Such standardization not only simplifies the integration of new modules but also ensures system compatibility and upgradeability regardless of future internal algorithmic optimizations. High-speed communication interfaces, such as Gigabit Ethernet and GTH (Giga-Transceiver High-speed), can be easily integrated, ensuring the necessary connectivity for raw key flow and post-processing data [19].

5. Conclusion

CV-QKD systems present significant computational challenges in post-processing, particularly during information reconciliation and privacy amplification. These operations demand high computational performance, numerical precision, and energy efficiency, which limits the adoption of generic architectures or commercial platforms in real-time and embedded quantum communication systems applications.

RISC-V's open and extensible ISA enables hardware specialization through custom instructions and dedicated co-processors for CV-QKD specific tasks, such as FFT-accelerated matrix operations for PA), parallel LDPC decoding for IR, and cryptographic hashing. This customization capability facilitates domain-optimized processors that simultaneously achieve adaptability, scalability, and energy efficiency for quantum-secure networks.

As next steps, we propose FPGA-based prototyping of RISC-V cores with CV-QKD instruction extensions, focusing on quantitative evaluation of throughput (Gbps), power efficiency (μW/bit), and protocol adaptability across diverse quantum channel conditions.

Acknowlegement

This work was fully funded by the project *HW DSP: Development and Prototyping of Multicore SoC with Dedicated Accelerators and RISC-V DSP*, supported by QuIIN – Quantum Industrial Innovation, the EMBRAPII CIMATEC Competence Center in Quantum Technologies. Financial resources were provided by the PPI IoT/Industry 4.0 program of the Brazilian Ministry of Science, Technology and Innovation (MCTI), under grant number 053/2023, in partnership with EMBRAPII.

References

[1] Xiaoyu Wu, Liang Liao, Xing Fan, Yuwei Chen, Jianyu Huang, Ming Liu, Zhen Tian, Ting Mu, Jiale Guo, Bo Liu, et al. A flexible soc for quantum key distribution post-processing based on risc-v processor. *Quantum Science and Technology*, 10(3):035027, 2025.

[2] David Harris and Sarah Harris. *Digital Design and*

Computer Architecture. Morgan Kaufmann, 2013.

[3] Valéria Loureiro da Silva, Micael Andrade Dias, Nelson Alves Ferreira Neto, and Alexandre B Tacla. From coherent communications to quantum security: Modern techniques in cv-qkd. In *2024 SBFoton International Optics and Photonics Conference (SBFoton IOPC)*, pages 1–5. IEEE, 2024.

[4] Nelson Alves Ferreira Neto, Joaquim Ranyere S. de Oliveira, Wagner Luiz A. de Oliveira, and João Carlos N. Bittencourt. Vlsi architecture design and implementation of a ldpc encoder for the ieee 802.22 wran standard. In *2015 25th International Workshop on Power and Timing Modeling, Optimization and Simulation (PATMOS)*, pages 71–76, 2015.

[5] Lucas Q. Galvão, Davi Juvêncio G. de Sousa, Micael Andrade Dias, and Nelson Alves Ferreira Neto. Neural network for excess noise estimation in continuous-variable quantum key distribution under composable finite-size security, 2025.

[6] R. Gallager. Low-density parity-check codes. *IRE Transactions on Information Theory*, 8(1):21–28, 1962.

[7] Roland Höller, Dominic Haselberger, Dominik Ballek, Peter Rössler, Markus Krapfenbauer, and Martin Linauer. Open-source risc-v processor ip cores for fpgas — overview and evaluation. In *2019 8th Mediterranean Conference on Embedded Computing (MECO)*, pages 1–6, 2019.

[8] Erfan Gholizadehazari, Tuba Ayhan, and Berna Ors. An fpga implementation of a risc-v based soc system for image processing applications. In *2021 29th Signal Processing and Communications Applications Conference (SIU)*, pages 1–4, 2021.

[9] Ruobing Han, Blaise Tine, Jaewon Lee, Jaewoong Sim, and Hyesoon Kim. Supporting cuda for an extended risc-v gpu architecture. *arXiv preprint arXiv:2109.00673*, 2021.

[10] Yaser Baseri, Vikas Chouhan, and Abdelhakim Hafid. Navigating quantum security risks in networked environments: A comprehensive study of quantum-safe network protocols. *Computers & Security*, 142:103883, 2024.

[11] Yichen Zhang, Yiming Bian, Zhengyu Li, Song Yu, and Hong Guo. Continuous-variable quantum key distribution system: Past, present, and future. *Applied Physics Reviews*, 11(1), 2024.

[12] Hans H Brunner, Chi-Hang Fred Fung, Momtchil Peev, Rubén B Méndez, Laura Ortiz, Juan P Brito, Vicente Martín, José M Rivas-Moscoso, Felipe Jiménez, Antonio A Pastor, et al. Demonstration of a switched cv-qkd network. *EPJ Quantum Technology*, 10(1):38, 2023.

[13] Xiaokang Wen, Qian Li, Haodong Mao, Xiaofeng Wen, and Ning Chen. An improved slice reconciliation protocol for continuous-variable quantum key distribution. *Entropy*, 23(10):1317, 2021.

[14] How Alice Outwits Eve. A talk on quantum cryptography. In *Coding Theory and Cryptography: From Enigma and Geheimschreiber to Quantum Theory*, page 144. Springer Science & Business Media, 2012.

[15] Fred Daneshgaran, Marco Mondin, and Kamran Olia. Permutation modulation for quantization and information reconciliation in cv-qkd systems. In *Quantum Communications and Quantum Imaging XV*, volume 10409, pages 61–70. SPIE, 2017.

[16] Xiaowei Wang, Yichen Zhang, Song Yu, and Hong Guo. High-speed implementation of length-compatible privacy amplification in continuous-variable quantum key distribution. *IEEE Photonics Journal*, 10(3):1–9, 2018.

[17] Enfang Cui, Tianzheng Li, and Qian Wei. Risc-v instruction set architecture extensions: A survey. *IEEE Access*, 11:24696–24711, 2023.

[18] Cristina Silvano, Daniele Ielmini, Fabrizio Ferrandi, Leandro Fiorin, Serena Curzel, Luca Benini, Francesco Conti, Angelo Garofalo, Cristian Zambelli, Enrico Calore, et al. A survey on deep learning hardware accelerators for heterogeneous hpc platforms. *ACM Computing Surveys*, 57(11):1–39, 2025.

[19] Samuel Greengard. Will risc-v revolutionize computing? *Communications of the ACM*, 63(5):30–32, 2020.