Secure Post-Processing in RISC-V for CV-QKD: Security Strategies with Hardware Security Module for Protection in FPGAs and ASICs

Leonardo Rodrigues Soares da Conceição[*,1], Paulo Cezar da Paixão[*,1], Wagner Luiz Alves de Oliveira[2], Calebe Micael de Oliveira Conceição[3], Nelson Alves Ferreira Neto[1]

[1]*QuIIN - Quantum Industrial Innovation, EMBRAPII CIMATEC Competence Center in Quantum Technologies, SENAI CIMATEC, Av. Orlando Gomes 1845, 41650-010, Salvador, BA, Brazil*

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

[3]*Computer Science Department, Federal University of Sergipe, 49100-000, São Cristóvão, SE, Brazil*

[*]*Corresponding authors: eng.leonardo.rodrigues@proton.me, engpcpx@proton.me*

Abstract: Continuous-variable quantum key distribution (CV-QKD) is a promising technology for secure communication in quantum networks, due to its compatibility with existing optical infrastructures and its potential for high key rates generation over metropolitan distances. Its deployment becomes increasingly feasible when integrated with reconfigurable hardware, such as field programmable gate arrays (FPGAs) or application-specific integrated circuits (ASICs), which enable performance optimization and architectural flexibility. However, the theoretical security of quantum protocols can be undermined by vulnerabilities in real hardware, especially during digital signal processing (DSP) and post-processing phases of key generation. This includes error correction (EC), information reconciliation (IR), and privacy amplification (PA). If implemented improperly, these steps may expose the system to physical and side-channel attacks (e.g., timing, power, or electromagnetic analysis), potentially leading to partial or full key leakage. This paper analyzes hardware design strategies to secure CV-QKD DSP and post-processing modules using custom fifth-generation Reduced Instruction Set Computing (RISC-V) processors. The main contribution is to emphasize the need for Hardware Security Modules (HSMs) embedded in the SoC, providing dedicated protection that general-purpose architectures cannot ensure. The proposed HSM safeguards cryptographic operations, enforces secure memory access, authenticates critical instructions, and ensures data integrity in real time. By combining the flexibility of RISC-V with the robustness of HSMs, this approach establishes a reliable and physically secure environment for embedded quantum key processing in future communication infrastructures.

Keywords: CV-QKD. RISC-V. FPGAs. ASICs. HSM.

1. Introduction

Quantum key distribution (QKD) enables secure communications based on the principles of quantum mechanics, allowing geographically separated parties to generate shared random binary keys with unconditional security [1, 2]. Between the QKD protocols, discrete-variable (DV-QKD) and CV-QKD stand out for their compatibility with existing optical infrastructures, integrating with coherent detection and digital signal processing (DSP) techniques[1].

A critical stage in CV-QKD systems is the post-processing phase, which transforms raw measurement data into usable cryptographic keys. This phase typically involves error correction, parameter estimation [3], and privacy amplification. To achieve flexibility and performance in executing these steps, a viable approach is to implement them on custom RISC-V processors deployed in digital logic hardware, such as FPGAs and ASICs.

The objective of this article is to analyze potential vulnerabilities in CV-QKD post-processing hardware modules implemented with custom RISC-V processors and to propose a protection strategy based on HSMs. The proposed architecture targets deployments on FPGAs and ASICs, aiming to pro-

vide a secure root of trust for embedded quantum key processing.

The structure of this paper is organized as follows: Section 2 provides the theoretical foundation of CV-QKD systems and RISC-V microarchitectures. Section 3 details hardware attack vectors targeting RISC-V microarchitectures. Section 4 introduces a security strategies for RISC-V microarchitectures using hardware security modules as a countermeasure. Section 5 discusses HSM integration models (external, integrated, ISA extensions). Section 7 evaluates HSM efficacy against side-channel attacks and their limitations. Section 8 describes the layered security architecture of HSMs (physical/logical protections). Section 9 presents the proposed HSM-integrated RISC-V architecture and concludes. Additional sections include acknowledgments and references.

2. Theoretical Foundation

A CV-QKD system consists of a transmitter (referred to as Alice), a quantum communication channel, and a receiver (called Bob) [1, 2]. Alice modulates coherent optical signals in both amplitude and phase, transmitting them through the optical channel. Bob receives these signals and measures them using coherent detection techniques, such as single or dual-quadrature measurements, detection, followed by a post-processing stage. The computational complexity of modern applications demands dedicated hardware for efficient execution [1]. Implementing operations on a RISC-V processor synthesized on an FPGA offers a flexible and efficient solution [2].

However, while CV-QKD protocols offer intrinsic security for the quantum communication channel, they do not inherently protect the classical hardware components of the system. As a result, hardware-based vulnerabilities remain exploitable, especially during post-processing. This motivates the adoption of secure hardware design strategies within digital circuits and RISC-V microarchitectures. One such strategy involves integrating HSMs into an FPGA or ASIC. These modules are designed to ensure the integrity, confidentiality, and robustness of critical operations, protecting sensitive data within RISC-V-based post-processing units from both physical and logical attacks.

2.1. The RISC-V Microarchitecture

The RISC-V microarchitecture refers to the specific physical implementation of the RISC-V ISA, an open technology developed by the University of California at Berkeley [4].

Central to its design, the pipeline structure of a RISC-V microarchitecture generally adheres to classic RISC principles, yet it presents substantial variation in implementation. In-order execution is common in embedded designs, typically featuring 3- to 5-stage pipelines. In contrast, high-performance implementations incorpo-

rate advanced techniques such as out-of-order execution, speculative branching, and multi-issue superscalar architectures. Memory hierarchies also vary widely – from simple physical memory addressing in microcontroller-class cores to complex, multi-level cache systems with coherence protocols in application-class processors.

The fundamental components of the microarchitecture include the following stages: (i) instruction fetch; (ii) instruction decoding; (iii) control unit; (iv) execution units – including the ALU, multiplication/division, and floating-point units; (v) memory subsystem – comprising caches and main memory; and (vi) flow control mechanisms for handling branches and exceptions.

This nature enables customization to meet specific requirements, but also introduces security challenges. CV-QKD implementations that utilize FPGAs and ASICs to accelerate cryptographic operations – particularly during the post-processing stages of communication – are especially vulnerable to attack techniques capable of extracting cryptographic keys. Consequently, analyzing potential attack vectors and implementing robust security strategies in digital circuit designs becomes a critical aspect of developing secure microarchitectures for quantum applications.

3. Attacks on RISC-V Microarchitectures

RISC-V microarchitectures are susceptible to side-channel attacks (SCAs), which exploit unintended information leakage during execution [5]. The architectural flexibility of RISC-V, while advantageous, can introduce specific vulnerabilities that can be exploited [6]. Notably, attacks targeting physical or behavioral characteristics of execution represent a significant threat. These will be discussed in the following, categorized by their primary exploitation mechanisms.

3.1. Power Analysis Attacks

Power analysis attacks involve monitoring the power consumption of a processor during cryptographic operations to infer sensitive information [7]. These attacks are typically classified into: (i) **Simple Power Analysis (SPA)**: Observes direct fluctuations in power consumption to reveal operational patterns; (ii) **Differential Power Analysis (DPA)**: Applies statistical methods across multiple executions to detect correlations and extract secret data; (iii) **Correlation Power Analysis (CPA)**: Computes the correlation between observed power traces and theoretical power consumption models, being effective against widely used cryptographic algorithms such as Advanced encryption standard (AES) and Data encryption standard (DES).

3.2. Electromagnetic Analysis

Electromagnetic Analysis is a non-invasive side-channel technique that captures electromagnetic emissions generated during cryptographic operations. These emissions can be detected using probes placed near the hardware, without requir-

ing any physical modification to the device [7].

3.3. Timing Attacks

Timing Attacks exploit variations in execution time to infer secret data. These variations may arise from: (i) differences in cache access latency; (ii) variations in modular multiplication timing; and (iii) non-constant-time crypto operations[7].

3.4. Memory Attacks

Memory Attacks target data remnants or unauthorized memory access pathways. Common techniques include: Cold Boot Attacks (exploit residual data in DRAM after power-off); DMA Attacks (use peripherals with direct memory access capabilities to read or modify memory without CPU intervention); and Thermographic Analysis (employ infrared imaging to capture heat patterns left by executed instructions, which can be analyzed and compared against known execution profiles of the target hardware) [7].

3.5. Speculative Attacks

Modern microarchitectures often implement speculative execution and branch prediction to improve performance by anticipating control flow and maximizing pipeline utilization. However, these same features introduce vulnerabilities that can be exploited through side-channel attacks, such as Spectre and Meltdown [8]. As high-performance RISC-V processors increasingly adopt these techniques, the security implications become more significant [6].

Such attacks can be used to gain unauthorized access to sensitive data residing in hardware components of a CV-QKD system. Therefore, implementing robust hardware-level protection strategies is essential to ensure the security and integrity of these quantum communication systems.

4. Countermeasures to Mitigate SCAs

To mitigate physical and logical attacks, specific countermeasures must be implemented at the microarchitectural level. One of the most effective approaches is the use of hardware security modules (HSMs) – dedicated devices designed to securely manage, protect, and process cryptographic material. HSMs establish a Trusted execution environment (TEE) [9] that isolates critical operations, ensuring confidentiality and integrity even under potential attack scenarios.

HSMs integrate physical protections such as intrusion detections systems and self-destruction mechanisms [10] and logical protections. These logical countermeasures employ specialized techniques to neutralize side-channel leakages, including:

4.1. Physical Protections

The physical layer constitutes the first line of defense for HSMs, incorporating robust mechanisms to deter and detect unauthorized access attempts. As demonstrated by [11], these devices integrate:

- **Advanced intrusion sensors**: Continuous monitoring for threats such as *fault injection* attacks (voltage/clock glitching, electromagnetic/laser injection) and environmental variations;

- **Secure key destruction**: Self-destruct circuits combined with Physical unclonable function (PUF) for volatile erasure of cryptographic material;

- **Emanations shielding**: TEMPEST protection with electromagnetic filtering and spectral spreading techniques;

- **Anti-tamper materials**: *Tamper-evident* enclosures and chemical component invalidation;

- **Physical Key Management**: Volatile storage via PUFs to eliminate data remanence and physical destruction upon intrusion detection (crypto-shredding);

4.2. Logical Protections

The logical layer implements techniques to mitigate software vulnerabilities, particularly against microarchitectural and side-channel exploitations. As detailed by [11], these mechanisms aim to neutralize threats exploiting:

- **Prevention of timing leaks**: The primary defense involves implementing constant-time operations, always executing the same number of clock cycles without conditional branches or memory accesses dependent on sensitive data.

- **Masking of cryptographic operations**: Involves injecting random values ("masks") into intermediate calculations to break the relationship between sensitive data and power profiles.

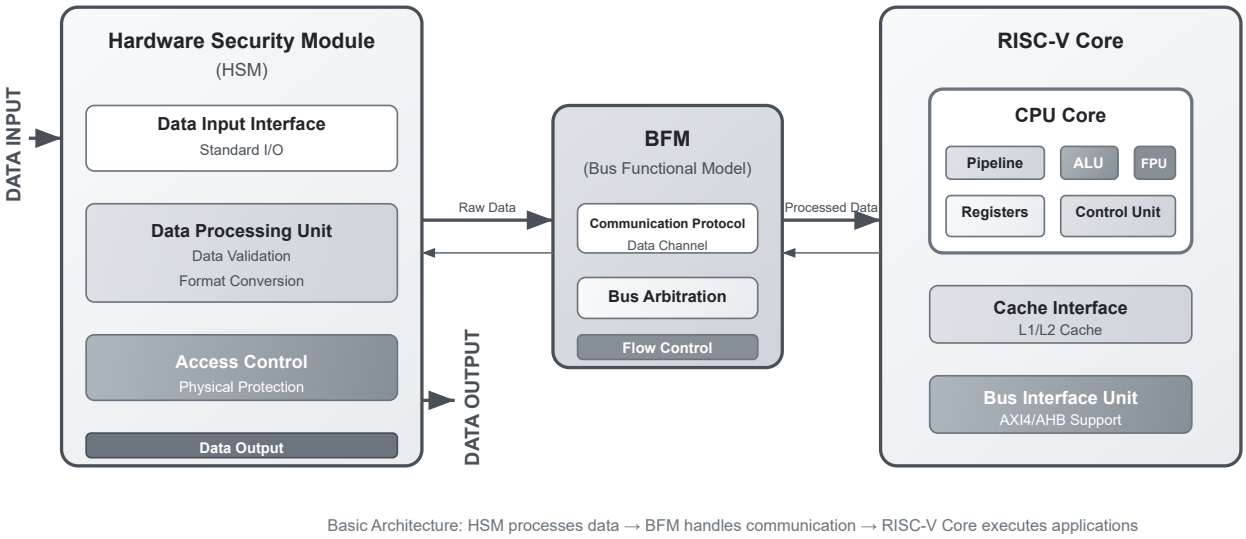
- **DVFS/RDFS to disrupt power analysis**: Protective measures implement dynamic and random voltage/frequency variations in the processor during sensitive operations. This degrades trace synchronization and dilutes statistical correlations.

- **Cache partitioning and granular memory encryption**: Attacks that induce bit flips in adjacent DRAM cells or extract data from memory after shutdown exploit unisolated access to shared memory. A solution involves processes where cache can be isolated into segments by security domain.

5. HSM integration on RISC-V Microarchitecture

The integration of hardware security modules into RISC-V systems can follow three main architectural models: (i) **External HSM**: Connected via standard interfaces such as PCIe, USB, or serial ports. This approach offers high flexibility and

Figure 1: RISC-V Microarchitecture with Integrated HSM via BFM



Source: Prepared by the authors.

modularity but introduces additional latency and may be less suitable for real-time or low-latency applications; (ii) **Integrated HSM**: Implemented as a coprocessor on the same silicon die as the RISC-V core. This model provides high performance and low latency, with tight coupling to the processor. However, it typically requires unified certification of the entire system, increasing design complexity and cost; and (iii) **Custom ISA Extensions**: Incorporates cryptographic operations and secure functions directly into the RISC-V instruction set architecture through custom extensions. This model achieves maximum integration and execution efficiency but may reduce portability and interoperability with standard RISC-V software ecosystems.

Hardware security modules constitute an effective countermeasure against side-channel attacks (SCAs) through: (i) constant-time execution; (ii) algebraic masking [12]; (iii) temporal randomization; and (iv) electromagnetic shielding.

Physical and logical protections present promising solutions that can be integrated into a RISC-V microarchitecture. However, given the challenges of quantum cryptography and quantum computing, it is crucial to maintaining security in quantum cryptographic systems. To address these threats, we proposed the integration of Hardware security modules (HSMs) with RISC-V cores by a Bus functional model (BFM), as illustrated in Figure 1. This architecture enhances both logical and physical security by facilitating secure communication channels and enabling hardware-level protection mechanisms. Such integration ensures robustness not only against classical attack vectors but also against emerging quantum threats.

6. Conclusion

This paper presented a comprehensive analysis of the security challenges in CV-QKD systems and the cryptographic key post-processing implemented within RISC-V hardware microarchitectures. It was examined the main types of attacks that can be executed on hardware platforms such as FPGAs and ASICs, including physical and side-channel attacks, such as power analysis, timing analysis, speculative execution exploits, and memory-based attacks. These vulnerabilities pose significant risks to the secure deployment of quantum-resistant systems in reconfigurable and dedicated hardware environments.

The main contribution of this work is to emphasize the necessity of integrating Hardware Security Modules (HSMs) when processors are employed for quantum key post-processing. HSMs provide a dedicated layer of hardware-based protection that mitigates vulnerabilities inherent to general-purpose or reconfigurable architectures, ensuring that post-processing operations remain secure even under advanced physical and side-channel attack scenarios.

In conclusion, the adoption of this architecture represents a promising path toward the development of trustworthy and long-lasting quantum communication systems. By combining the flexibility of RISC-V with the robustness of HSMs for secure platforms capable of withstanding both current and future cyber threats.

Acknowledgement

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] V. L. da Silva, M. A. Dias, N. A. F. Neto, and A. 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, Salvador, Brazil, 2024. IEEE.

[2] Cosmo Lupo, Carlo Ottaviani, Panagiotis Papanastasiou, and Stefano Pirandola. Continuous-variable measurement-device-independent quantum key distribution: Composable security against coherent attacks. *Physical Review A*, 97(5):052327, 2018.

[3] 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.

[4] Andrew Waterman, Yunsup Lee, David A. Patterson, and Krste Asanović. The risc-v instruction set manual, volume i: User-level isa, version 2.0. Technical Report UCB/EECS-2014-54, EECS Department, University of California, Berkeley, 2014.

[5] Mahya Morid Ahmadi, Faiq Khalid, and Muhammad Shafique. Side-channel attacks on risc-v processors: Current progress, challenges, and opportunities. In *Proceedings of the Fifth International Conference on Cyber-Technologies and Cyber-Systems*, pages 1–6. ThinkMind, 2020.

[6] Lukas Gerlach, Daniel Weber, Ruiyi Zhang, and Michael Schwarz. A security risc: Microarchitectural attacks on hardware risc-v cpus. In *IEEE Symposium on Security and Privacy (S&P)*, 2023.

[7] Abolfazl Sajadi, Nusa Zidaric, Todor Stefanov, and Nele Mentens. A systematic comparison of side-channel countermeasures for risc-v-based socs. In *Proceedings of NorCAS 2024*, pages 1–6, 2024.

[8] Paul Kocher, Jann Horn, Anders Fogh, Daniel Genkin, Daniel Gruss, Werner Haas, Mike Hamburg, Moritz Lipp, Stefan Mangard, Thomas Prescher, Michael Schwarz, and Yuval Yarom. Spectre attacks: Exploiting speculative execution. In *2019 IEEE Symposium on Security and Privacy (SP)*, pages 1–19. IEEE, 2019.

[9] Lamya Abdullah. Physical security devices for computer subsystems: A survey of attacks and defenses. Thesis, 2021.

[10] Mike Bond and Ross Anderson. Api-level attacks on embedded systems. *Computer*, 34(10):67–75, 2001.

[11] Modern hardware security: A review of attacks and countermeasures. *arXiv preprint arXiv:2501.04394*, 2025.

[12] Suresh Chari, Charanjit S. Jutla, Josyula R. Rao, and Pankaj Rohatgi. Towards sound approaches to counteract power-analysis attacks. In *Advances in Cryptology — CRYPTO' 99*, volume 1666 of *Lecture Notes in Computer Science*, pages 398–412. Springer-Verlag, 1999.