TYRCA: A RISC-V Tightly-coupled accelerator for Code-based Cryptography

Alessandra Dolmeta[3,1], Stefano Di Matteo[1,2]*, Emanuele Valea[2], Mikael Carmona[1], Antoine Loiseau[1], Maurizio Martina[3] and Guido Masera[3]

[1]Univ. Grenoble Alpes, CEA, LETI, F-38000 Grenoble, France, [2]Univ. Grenoble Alpes, CEA, LIST, F-38000 Grenoble, France, [3]DET, Politecnico di Torino, Torino, Italy

Abstract

*Post-quantum cryptography (PQC) has garnered significant attention across various communities, particularly with the National Institute of Standards and Technology (NIST) advancing to the fourth round of PQC standardization. One of the leading candidates is Hamming Quasi-Cyclic (HQC), which received a significant update on February 23, 2024. This update, which introduces a classical dense-dense multiplication approach, has no known dedicated hardware implementations yet. The innovative Core-V eXtension InterFace (CV-X-IF) is a communication interface for RISC-V processors that significantly facilitates the integration of new instructions to the Instruction Set Architecture (ISA), through tightly connected accelerators. In this paper, we present a **T**ightl**Y**-coupled accelerator for **R**ISC-V for **C**ode-based cryptogr**A**phy (TYRCA), proposing the first fully tightly-coupled hardware implementation of the HQC-PQC algorithm, leveraging the CV-X-IF. The proposed architecture is implemented on the Xilinx Kintex-7 FPGA. Experimental results demonstrate that TYRCA reduces the execution time by 94% to 96% for HQC-128, HQC-192, and HQC-256.*

Introduction

Quantum computers promise transformative advancements in fields such as medicine, materials science, and AI, but they also threaten current communication security by undermining cryptosystems like RSA, Diffie-Hellman, and ECC, which are vulnerable to quantum attacks. To address this, the National Institute of Standards and Technology (NIST) has been leading efforts to standardize Post-Quantum Cryptography (PQC) algorithms, resistant against quantum computing attacks. Among these, code-based cryptography, including schemes like Classic McEliece, BIKE, and HQC, has emerged as a strong contender. HQC, the focus of this paper, utilizes structured codes and the complexity of decoding random quasi-cyclic codes in the Hamming metric. Current HQC implementations are either fully hardware-based or use loosely coupled accelerators for specific algorithm components. Fully hardware-based approaches offer superior performance but come with a fixed implementation footprint and limited flexibility. Loosely coupled accelerators, while more versatile and capable of serving multiple applications, impose significant costs on System-on-Chip (SoC) designers due to integration challenges and the need for custom software drivers. Tightly coupled acceleration has gained traction, particularly with the rise of the RISC-V standard, which supports custom ISAs in an open-source framework. However, implementing tightly coupled accelerators requires modifications to the CPU and the compilation toolchain. In this work, we overcome these limitations by using a novel approach for tightly coupled acceleration that is being standardized in the RISC-V community: the Core-V eXtension InterFace (CV-X-IF)[1]. This interface offers a seamless way to support tightly-coupled accelerators by enhancing the CPU with custom or standardized instructions, without modifying the pipeline of the CPU. In this work, we show how the CV-X-IF interface facilitates smooth integration with a RISC-V CPU core for implementing cryptographic tasks and we provide TYRCA, the first CV-X-IF-based tightly coupled implementation of round-4 HQC. The proposed architecture has been deployed on FPGA to show area and performance results.

TYRCA and System Integration

HQC [1] is a Key Encapsulation Mechanism (KEM) that relies on the hardness of the syndrome decoding problem in linear quasi-cyclic codes. The HQC KEM is composed of three functions: Key Generation (KeyGen), Encapsulation (Encaps), and Decapsulation (Decaps). HQC is available in three different security levels, namely HQC-128, HQC-192, and HQC-256, each with a different parameter set. We conducted a profiling of HQC-128 on the 32-bit SoC of Figure 1. We considered the latest version of HQC software compiled with optimization level `-O2`. As reported in Table 1, the execution time of the HQC algorithm is significantly influenced by the arithmetic in $\mathcal{R}$ (polynomial ring). Keccak, though minimally contributing, is consistently used in the algorithm. The Reed-Solomon

*Corresponding author: `stefano.dimatteo@cea.fr`

[1] `https://github.com/openhwgroup/core-v-xif/tree/main`

and Reed-Muller (RS-RM) codes, particularly encoding and decoding, present notable bottlenecks during encapsulation and decapsulation, contributing up to 5% of the total execution time.

Table 1: *Kcycles of the main sub-functions of HQC-128*

Function	KeyGen	Encaps	Decaps
Total	**66,026**	**133,331**	**208,550**
Arith. in $\mathcal{R}$	64,603	129,206	193,809
Keccak	27	83	81
RS-RM Code	-	995	10

To accelerate the bottlenecks just mentioned, we designed TYRCA, a hardware accelerator for HQC connected to a CV32E40PX processor through the CV-X-IF. The architecture of the proposed SoC and TYRCA is reported in Figure 1. TYRCA is mainly composed of the CV-X-IF controller and three accelerators: the $\mathcal{R}$-Unit, RS-decoder, and Keccak. Each of these accelerators is customized to execute one or more specific instructions. The CV-X-IF interface is connected directly to the register file of the CPU.

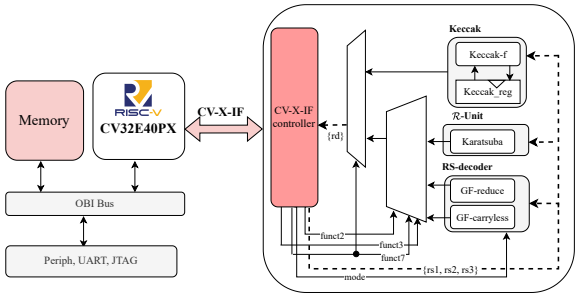

Figure 1: *SoC architecture plus TYRCA accelerator*

The $\mathcal{R}$-Unit computes a Karatsuba multiplication. The original implementation in HQC uses a bitwise Karatsuba multiplication algorithm for 64-bit integers. Our version operates on 32-bit integers, breaking each 64-bit integer into two 32-bit chunks. The accelerator supports four custom instructions and it includes a carry-less multiplier along with the necessary logic to manage inputs, manage outputs (reconstruction module), store intermediate results, and perform XOR operations. The RS-decoder module accelerates two atomic functions: the GF-reduce (Galois-Field-reduce) function, which reduces a polynomial x modulo a given primitive polynomial, implemented with three customized instructions; the GF-carryless, which performs carry-less multiplications of two 8-bit polynomials storing the result in a 16-bit polynomial. The proposed implementation uses four custom instructions to perform carry-less multiplication directly on TYRCA. The Keccak accelerator features a 1600-bit state register and performs 24 rounds of the five Keccak transformations [2]: θ, ρ, π, χ, and ι. Keccak is the only TYRCA accelerator equipped with a dedicated register and requires numerous load and store instructions to fill its internal register. However, the overhead from the load/store process with the CV-X-IF is less than the overhead that would result from using the Keccak accelerator in loosely coupled mode. In this case, we have shown that the CV-X-IF has significant potential for multi-cycle operations as well. Three custom instructions have been introduced: a specialized `store` operation to upload the state register; a `start` instruction to initiate the 24-round process; and a `load` operation to save the result back to the core's register file.

Results

The SoC of Figure 1 has been implemented on the Xilinx Kintex-7 FPGA. The results in Table 2 illustrate a substantial decrease in clock cycles with the optimized TYRCA implementation compared to the original SW implementation. Across all security levels—HQC-128, HQC-192, and HQC-256—the TYRCA implementation achieves approximately a 95% reduction in clock cycles for KeyGen, Encaps, and Decaps.

Table 2: *Kcycles and performance gain with TYRCA*

Version	Level	KeyGen	Encaps	Decaps
SW [1]	128	66,026	133,331	208,550
	192	195,307	392,977	600,490
	256	357,245	719,137	1,106,009
TYRCA	128	3,108 [-95.29%]	6,302 [-95.27%]	11,095 [-94.68%]
	192	10,847 [-95.22%]	22,578 [-95.27%]	34,895 [-94.97%]
	256	20,153 [-95.06%]	41,469 [-95.13%]	64,999 [-94.82%]

Conclusion

In this work, we propose TYRCA, a tightly-coupled acceleration solution for RISC-V architectures based on the CV-X-IF, that offers a seamless integration for extending RISC-V ISA. Experimental results confirm TYRCA's effectiveness, achieving an execution time reduction of 94% to 96% across HQC-128, HQC-192, and HQC-256.

Acknowledgement

This work received funding from the French National Research Agency under G.A. ANR-22-PETQ-0008 PQ-TLS and from SERICS (PE00000014) under the PNRR MUR funded by the NextGenerationEU.

References

[1] C. A. Melchor et al. *Hamming Quasi-Cyclic (HQC) Fourth Round Version*. Online. Updated version 23/02/2024. 2024. URL: `https://pqc-hqc.org/documentation.html`.

[2] Quynh Dang et al. *Secure hash standard*. 2015.