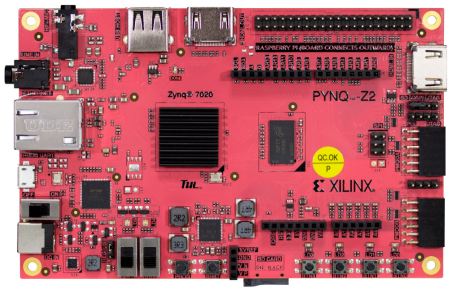
Hardware Acceleration of Fully Homomorphic Encryption on Edge Devices



Fully Homomorphic Encryption (FHE) is a cryptographic technique that enables computations to be performed directly on encrypted data without requiring decryption. This allows sensitive data to remain confidential throughout the computation process and makes FHE attractive for privacy-critical applications such as cloud computing, medical data analysis, and privacy-preserving machine learning.

While most research on FHE focuses on accelerating computations on encrypted data in cloud environments, practical deployments also require data to be encrypted directly on edge devices such as IoT sensors or mobile devices. In these settings, encryption must operate under strict constraints in terms of computational power, memory, and energy consumption. Although FHE encryption is cheaper than homomorphic evaluation, existing implementations are typically designed for powerful desktop or server processors and are not optimized for constrained hardware.

This thesis investigates efficient implementations of FHE encryption on edge devices using the Xilinx PYNQ platform as an embedded hardware environment. The student will analyze the computational and memory bottlenecks of the encryption process and explore optimization techniques suited for constrained hardware. By leveraging both the ARM processor and programmable logic on the PYNQ board, the goal is to design and implement an efficient encryption pipeline for edge devices.

We are looking for a student with an interest in cryptography and hardware/software co-design. The project will involve implementing the encryption procedure of an FHE scheme using C and Verilog on the Xilinx PYNQ platform. The student will design and evaluate an efficient encryption pipeline and provide insights into the feasibility of performing FHE encryption directly on constrained hardware platforms.

Practicalities

Promotor:	Ingrid Verbauwhede		
Daily supervisor:	Xander Pottier	xander.pottier@esat.kuleuven.be	office 01.21
	Zetao Miao	zetao.miao@esat.kuleuven.be	office 01.23

Nature of the work:	15% literature, 75% software/hardware, 10% writing
Number of students:	1

 © 2026 – 2027 COSIC