

# Emulador de algoritmos cuánticos implementado en FPGA utilizando herramientas de Alto Nivel

Universidad Nacional de Mar del Plata.



Agustin Silva



I C Y T E



Introducción

# Algoritmos Cuánticos

(*versus* Algoritmos Clásicos)



# Emulador

(*versus* Simulador)



# FPGA

(*versus* MicroProcesador)

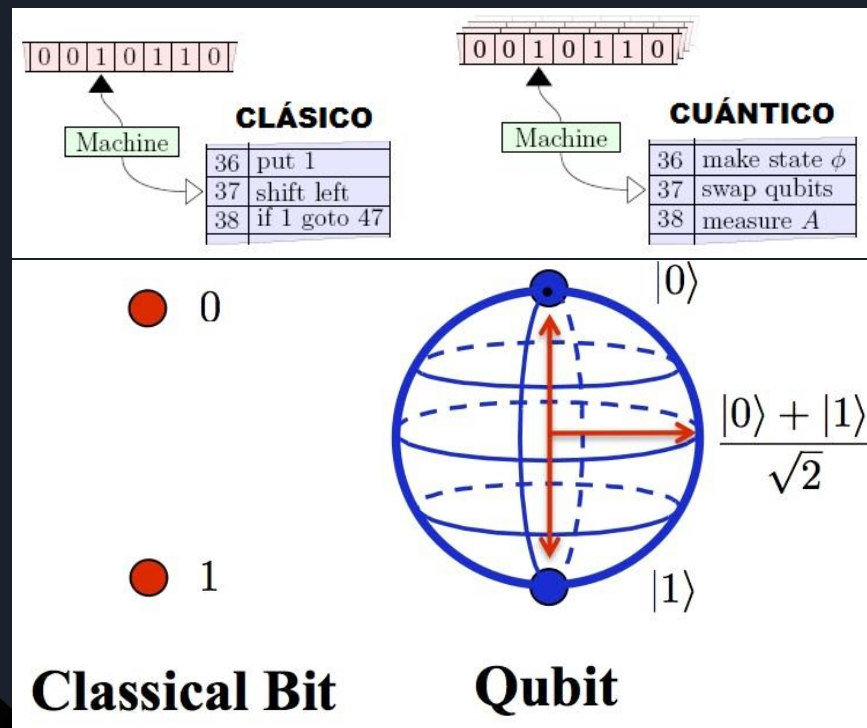


# Alto Nivel

(*versus* Bajo Nivel)

# Computación Cuántica. Representación de algoritmos e información.

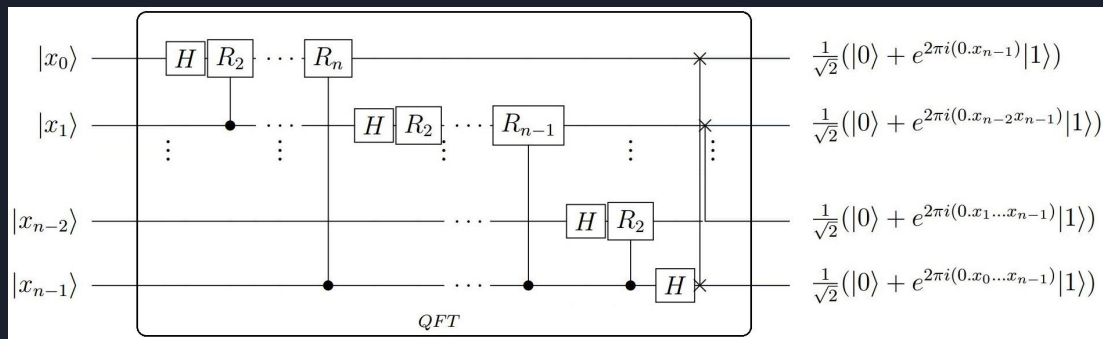
Marco Teórico



# Transformada cuántica de Fourier (QFT).

## Representación circuital y matricial.

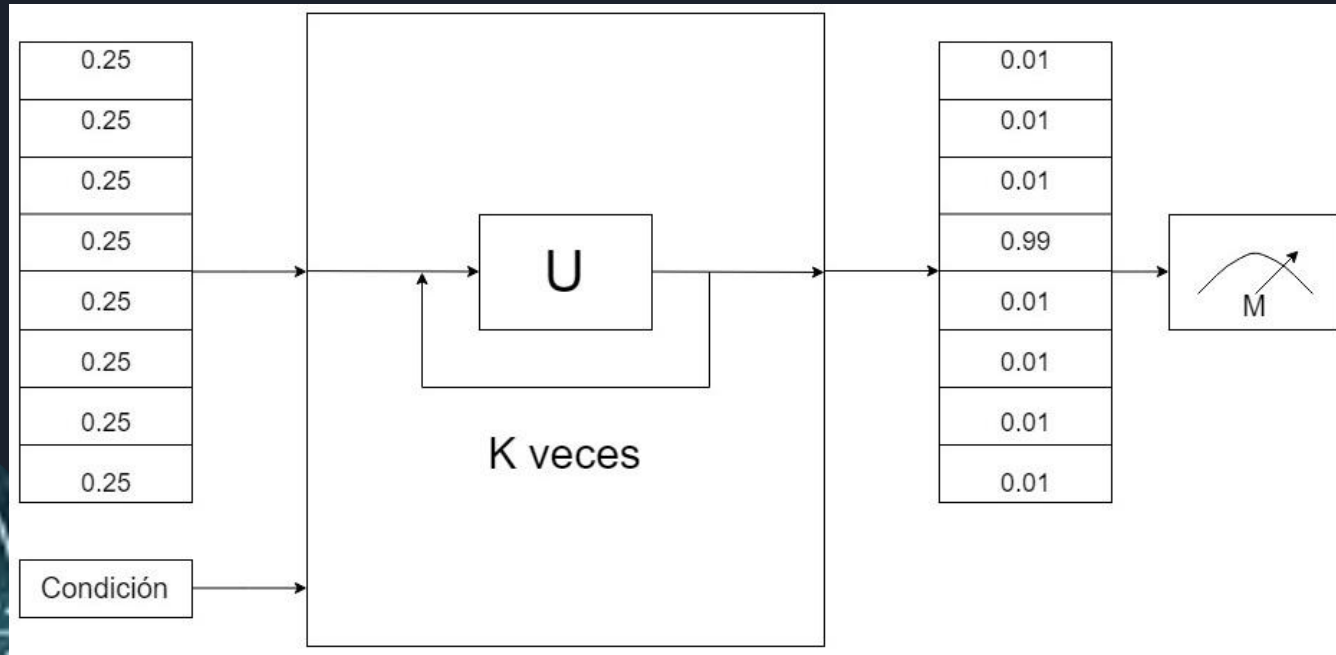
Marco Teórico



$$M^{QFT} = \frac{1}{\sqrt{N}} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & w & w^2 & \dots & w^{N-1} \\ 1 & w^2 & w^4 & \dots & w^{2(N-1)} \\ 1 & \vdots & \vdots & \dots & \vdots \\ 1 & \vdots & \vdots & \dots & \vdots \\ 1 & w^{N-1} & w^{2(N-1)} & \dots & w^{(N-1)(N-1)} \end{bmatrix} \quad w = e^{\frac{2\pi i}{N}}$$

# Algoritmo de Grover. Algoritmo de búsqueda. Enfoque cuántico.

Marco Teórico

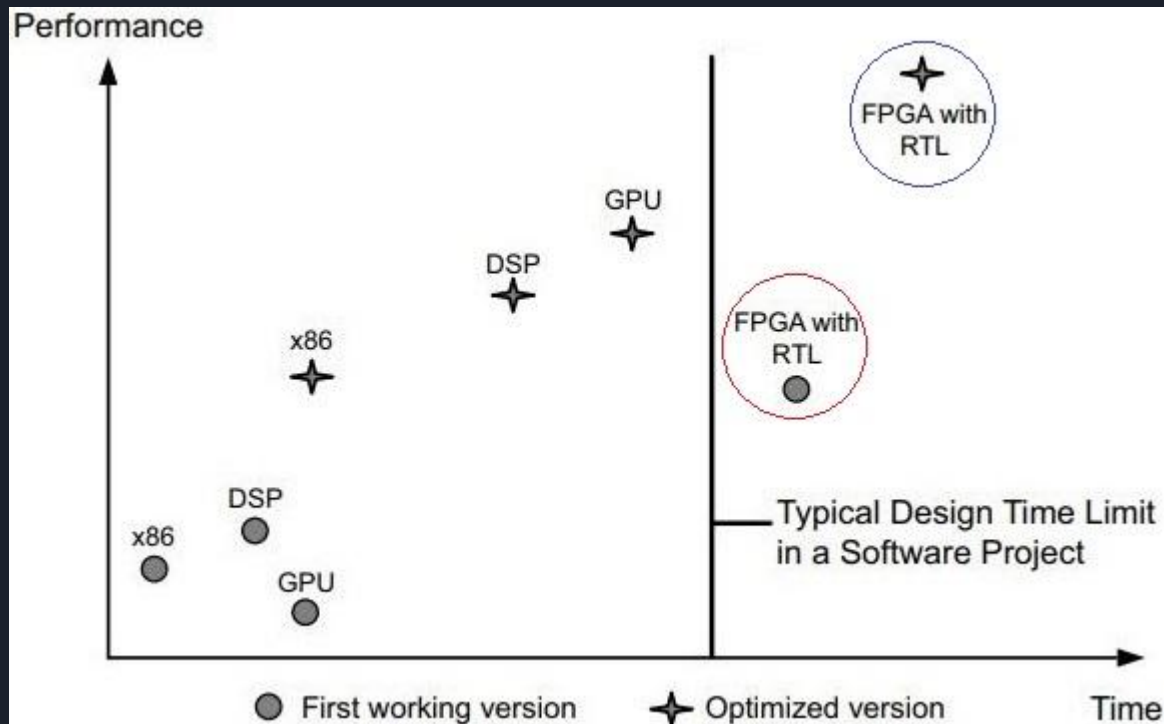




VIVADO ©.

# Performance vs Tiempo de Diseño

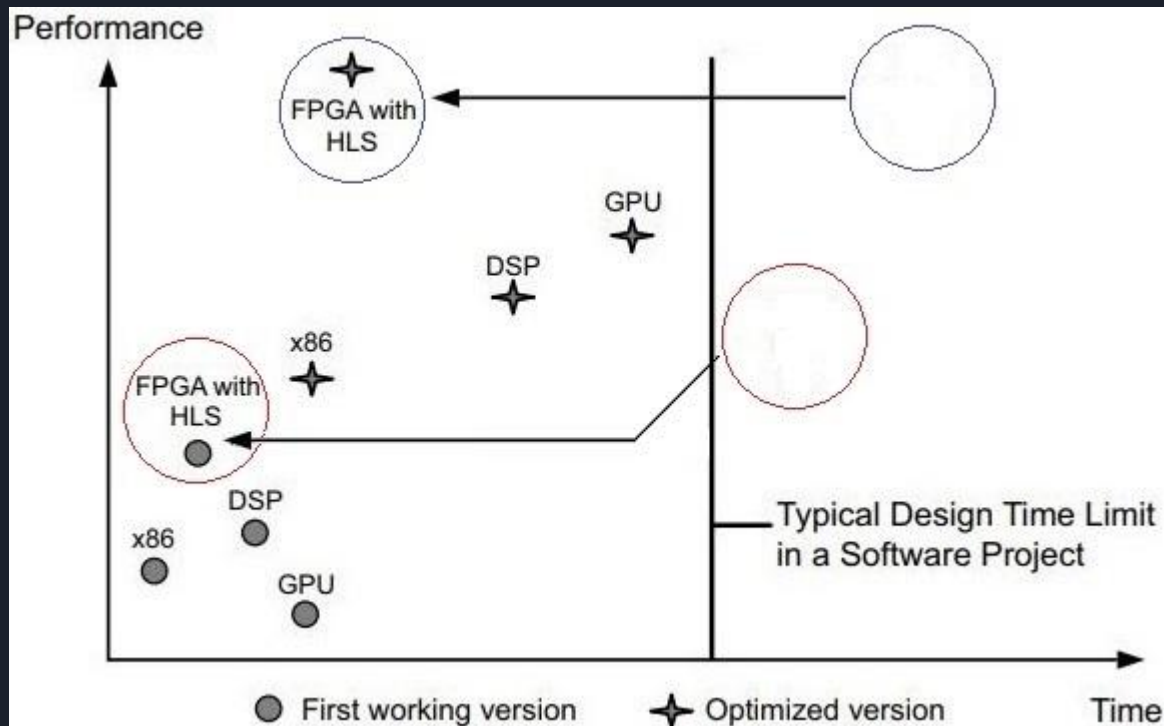
Implementación



VIVADO ©.

# Performance vs Tiempo de Diseño

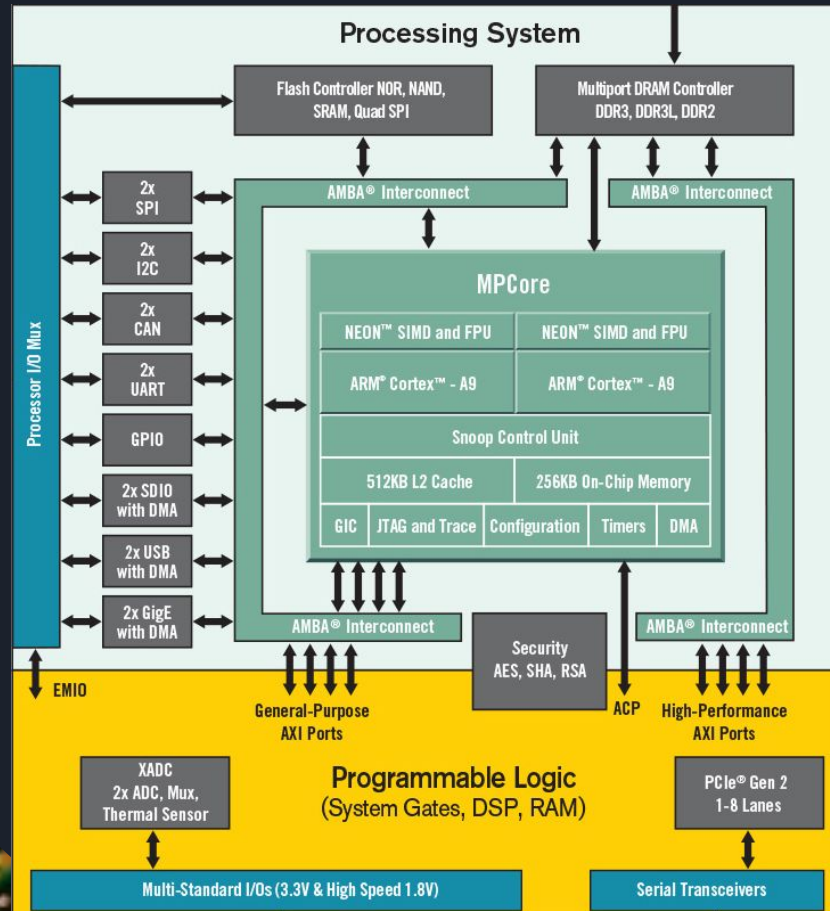
Implementación



# Esquema del Chip Zynq 7000 (SoC).

PS (ARM® Cortex™-A9).

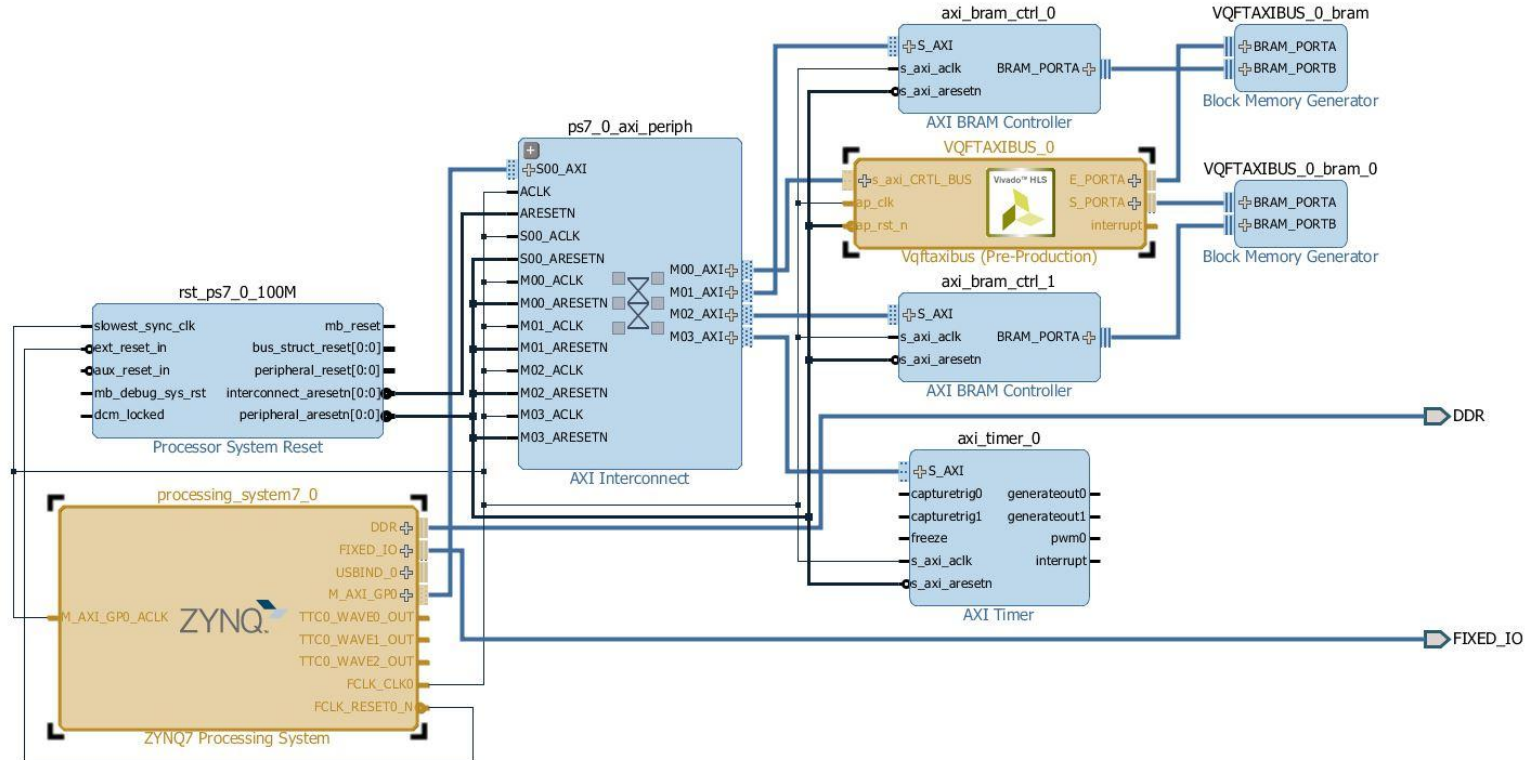
## Implementación



PL (arreglo de compuertas). 11

# Diagrama en bloques del Emulador.

# Implementación

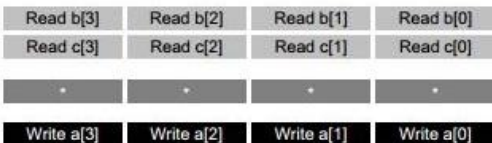


Directivas según la naturaleza del algoritmo.

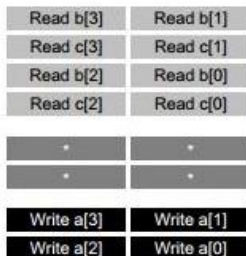
## Transformada de Fourier

```
void top(...) {
    ...
    for_mult:for (i=3;i>0;i--) {
        a[i] = b[i] * c[i];
    }
    ...
}
```

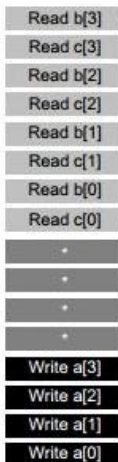
Rolled Loop



Partially Unrolled Loop



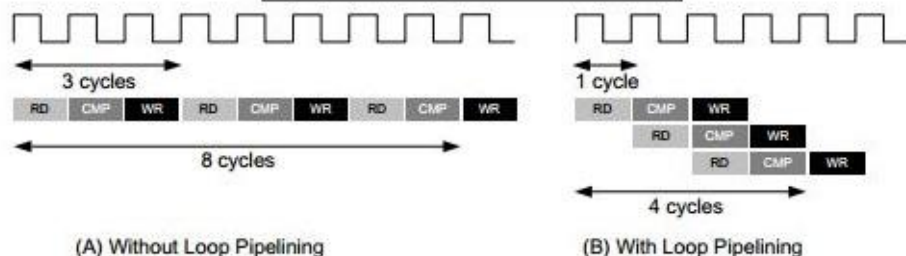
Unrolled Loop



## Implementación

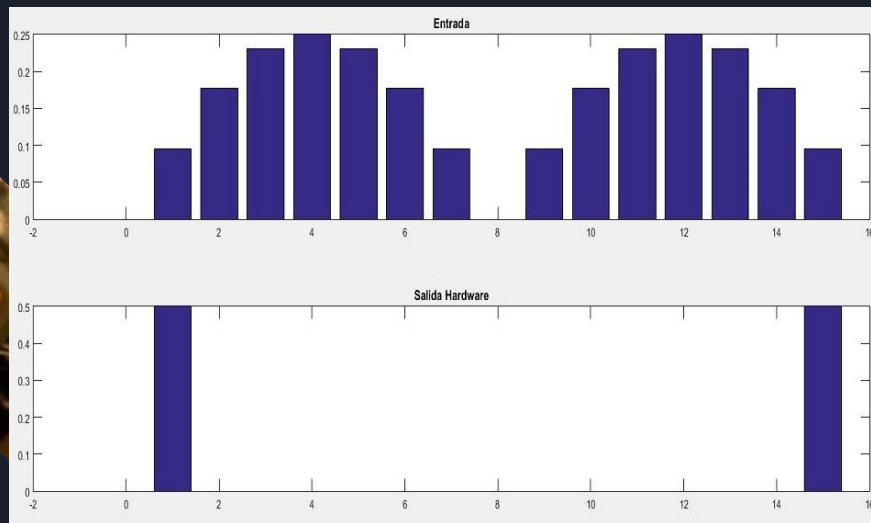
## Algoritmo de Grover

```
void func(m,n,o) {
    for (i=2;i>=0;i--) {
        op_Read;
        op_Compute;
        op_Write;
    }
}
```

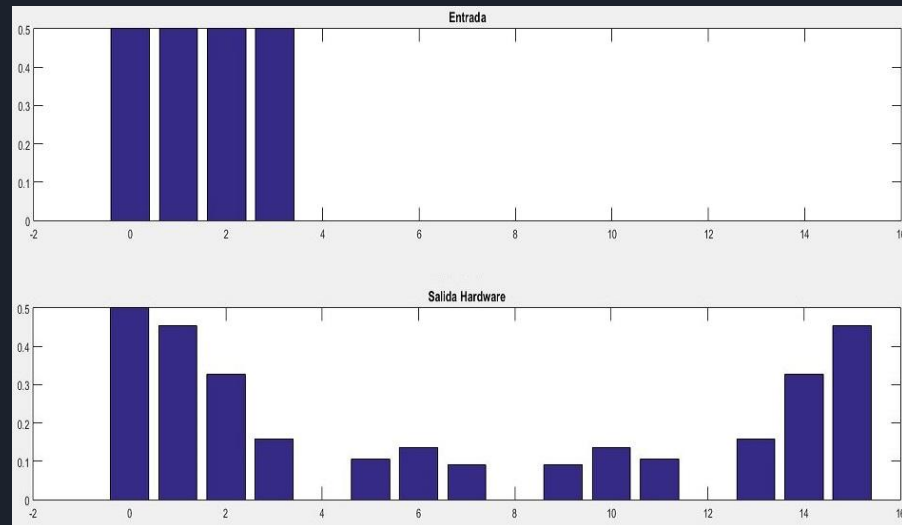


# Eficacia del Emulador. Transformada cuántica de Fourier.

## Análisis de Resultados



Entrada senoidal

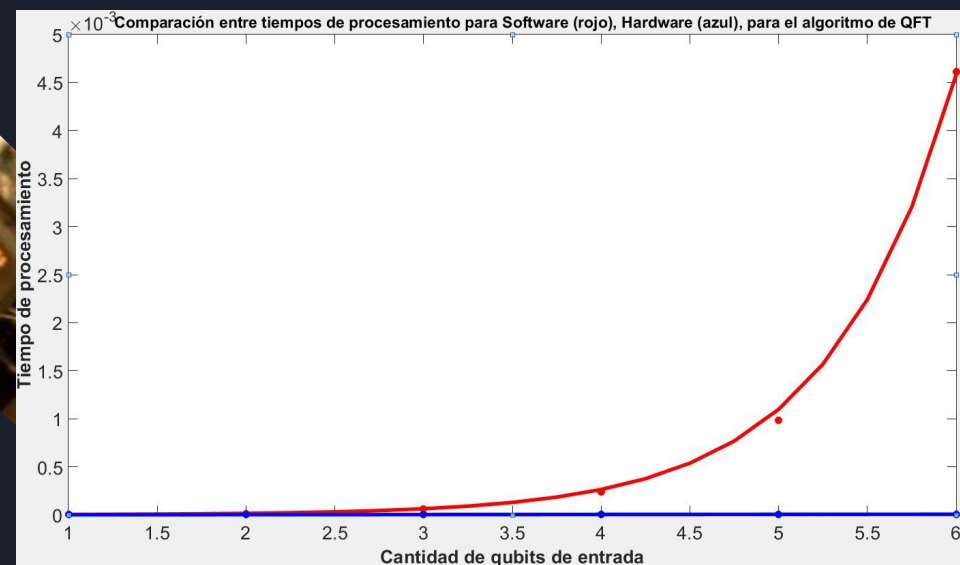


Entrada pulsante

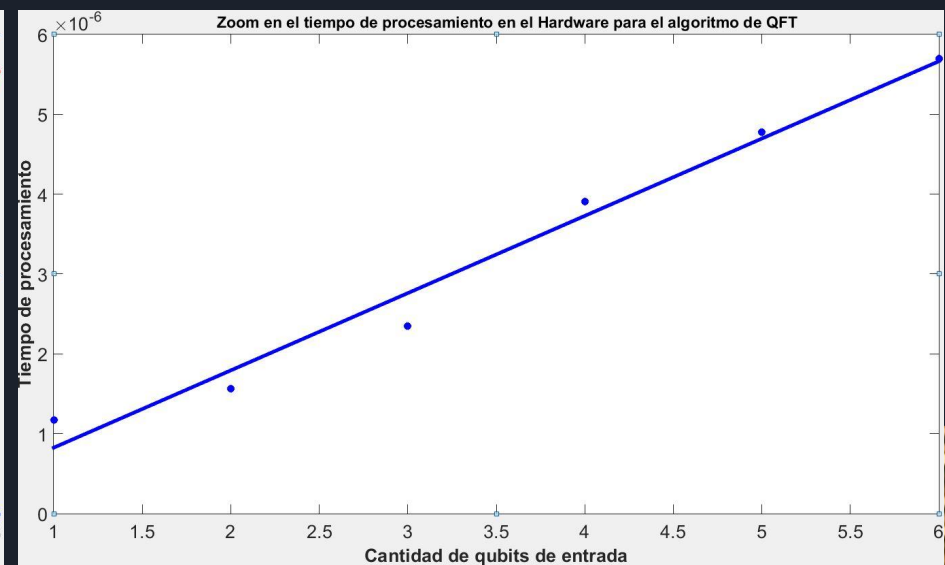
# Eficiencia del Emulador. Transformada cuántica de Fourier.

## Análisis de Resultados

### FPGA vs MicroProcesador



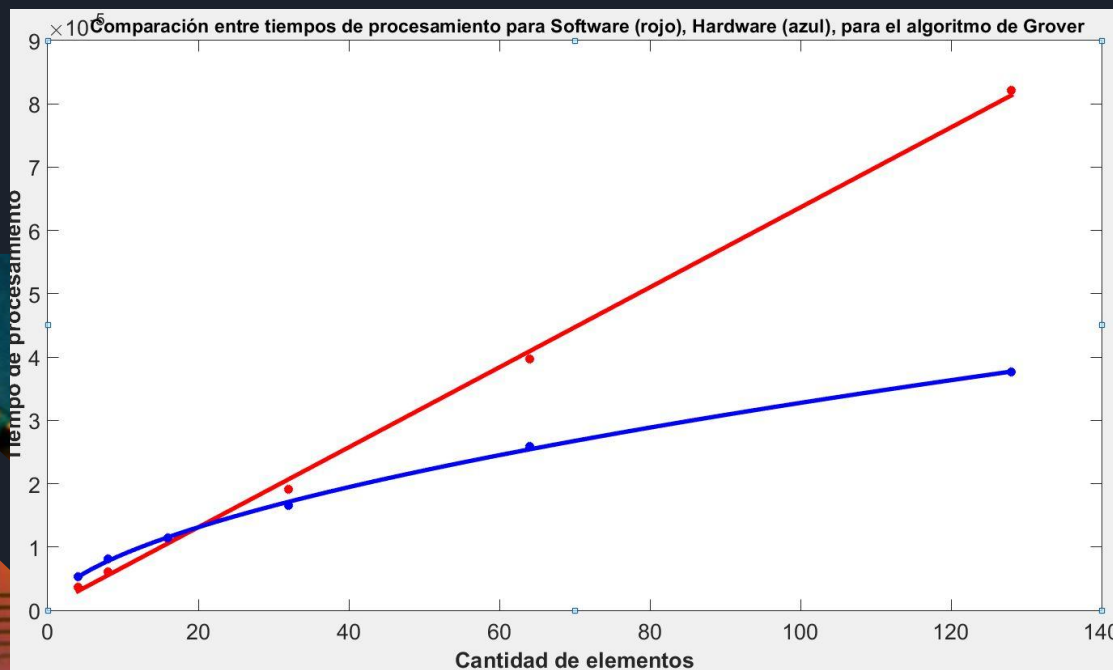
### Zoom en FPGA





# Eficiencia del Emulador. Algoritmo de búsqueda de Grover.

## Análisis de Resultados



FPGA vs MicroProcesador.



Emulador de algoritmos cuánticos implementado  
en FPGA utilizando herramientas de Alto Nivel

Conclusiones

→ MODELABLE

Emuladores en FPGA pueden imitar la **naturaleza  
paralelística** de la computación cuántica.



Emulador de algoritmos cuánticos implementado  
en FPGA utilizando herramientas de Alto Nivel

Conclusiones

→ MODELABLE  
→ ACCESIBLE

La programación de Hardware a través de  
herramientas de **Alto Nivel** resulta más  
abordable para los investigadores.



Emulador de algoritmos cuánticos implementado  
en FPGA utilizando herramientas de Alto Nivel

Conclusiones

→ MODELABLE  
→ ACCESIBLE  
→ FLEXIBLE

El diseño de algoritmos para este emulador permite  
**modificar el sistema** fácilmente, a diferencia de los  
realizados con lenguaje de bajo nivel.



Emulador de algoritmos cuánticos implementado  
en FPGA utilizando herramientas de Alto Nivel

Conclusiones


→ MODELABLE  
→ ACCESIBLE  
→ FLEXIBLE  
→ VELOZ

El tiempo de procesamiento baja notablemente  
junto con una disminución en el orden de  
crecimiento.





- El costo de la disminución en el tiempo de procesamiento es un aumento exponencial en la cantidad de hardware necesario.



Emulador de algoritmos cuánticos implementado  
en FPGA utilizando herramientas de Alto Nivel

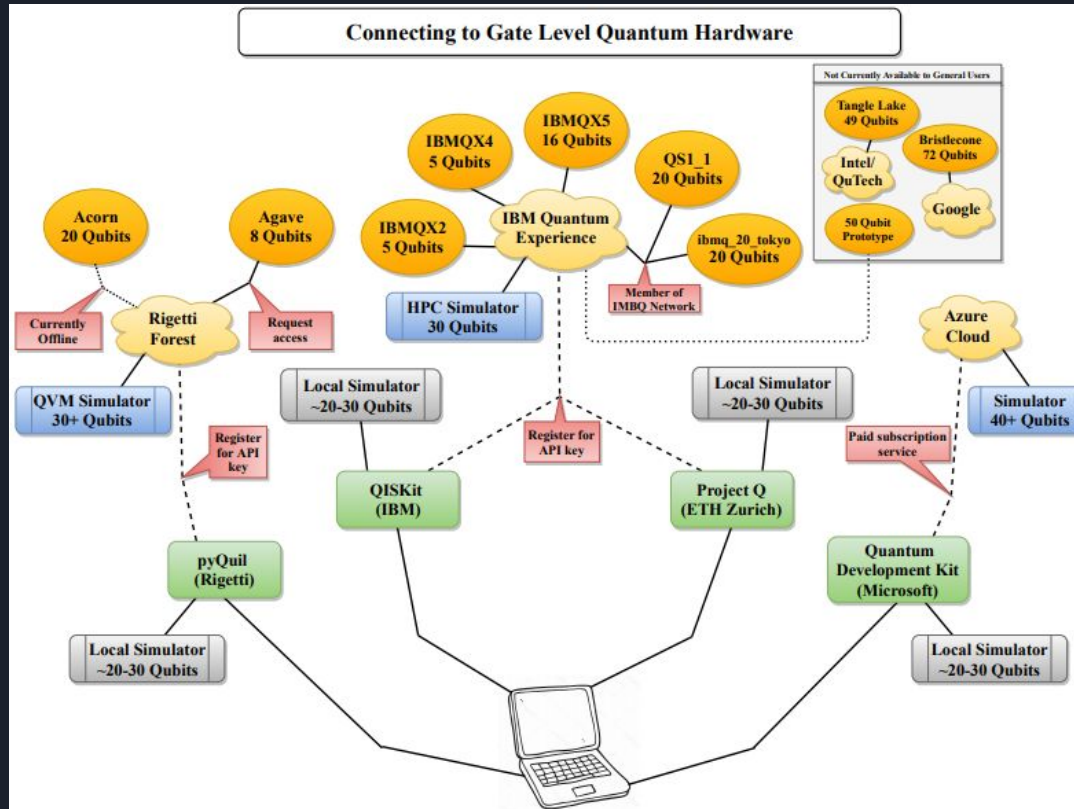
**TRABAJO EN DESARROLLO:** 'Intercambio de información y algoritmos cuánticos para el diseño y modelado de sistemas de comunicación'

- Simular algoritmos, circuitos y sistemas cuántos complejos en software desarrollado:

**Forest** (Rigetti), **QISKit** (IBM),  
**ProjectQ** (ETH Zurich), **QDK**  
(Microsoft), **Cirq** (Google), etc

# Emulador de algoritmos cuánticos implementado en FPGA utilizando herramientas de Alto Nivel

Trabajos a futuro



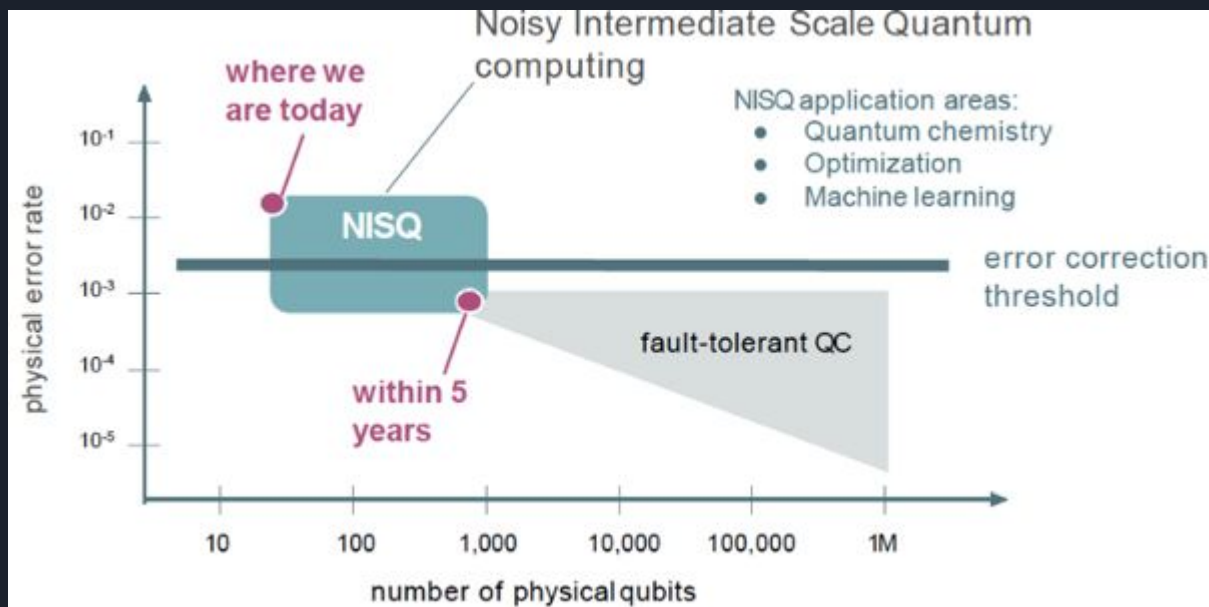




Emulador de algoritmos cuánticos implementado  
en FPGA utilizando herramientas de Alto Nivel

Trabajos a  
futuro

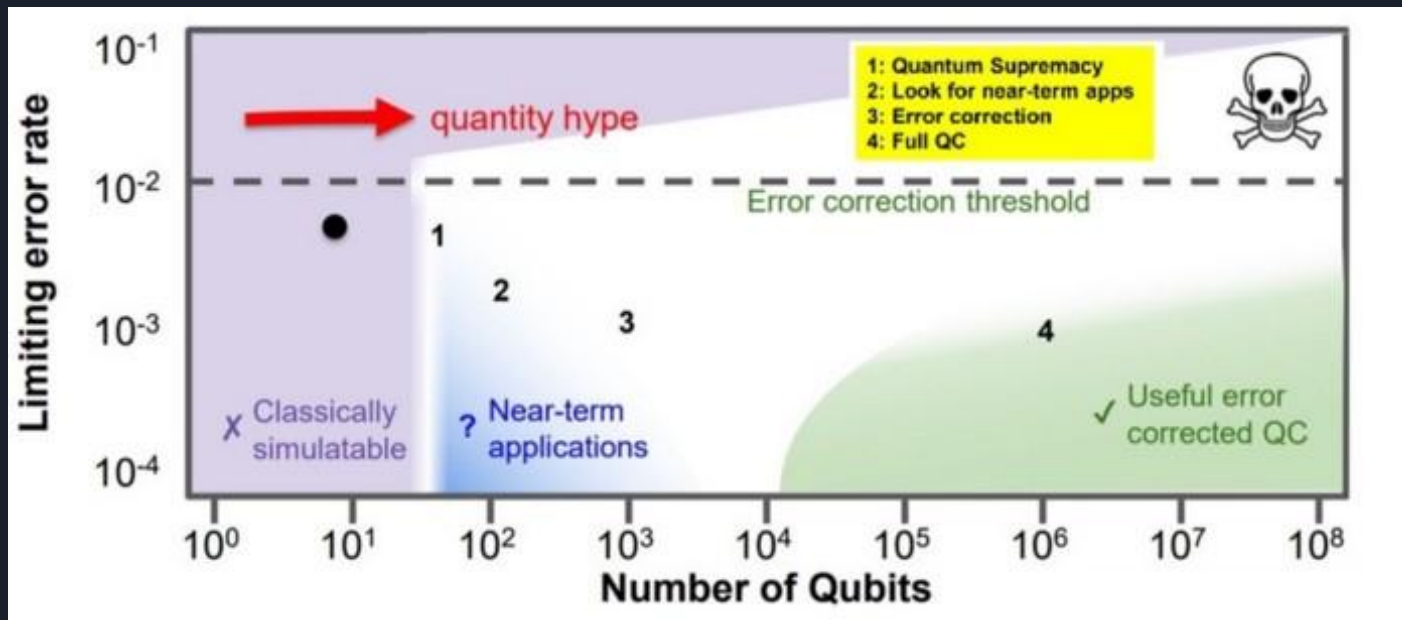
- Probar algoritmos en las **NISQ** desarrolladas






Emulador de algoritmos cuánticos implementado  
en FPGA utilizando herramientas de Alto Nivel

Trabajos a  
futuro



- Estudiar y diseñar algoritmos de criptografía:
  - Cuánticos (BB84, E91, SARG04, KMB09)
  - Post-cuánticos (NIST)

The background is a dark navy blue. In the top-left corner, there are two overlapping parallelogram shapes, one blue and one light green. In the bottom-left, there is a circular inset showing a detailed, grayscale image of a printed circuit board (PCB) with various electronic components. In the top-right corner, there is a grayscale image of a complex, multi-layered circuit board structure. The text 'PREGUNTAS' and a question mark are centered on the right side of the image.

# PREGUNTAS

?

The background is a dark navy blue. In the top-left corner, there are two overlapping geometric shapes: a blue parallelogram and a light green parallelogram. In the bottom-left corner, there is a circular inset showing a detailed, grayscale image of a printed circuit board (PCB) with various electronic components. In the top-right corner, there is a grayscale image of a complex, multi-layered circuit board structure. The text "MUCHAS GRACIAS" is centered in the middle-right portion of the image.

MUCHAS  
GRACIAS