



UNIVERSIDAD NACIONAL DEL ALTIPLANO PUNO

FACULTAD DE INGENIERIA ESTADISTICA E
INFORMATICA

**USO DE PROCESADORES DE TARJETAS GRÁFICAS
PARA LA VALIDACIÓN DE FORTALEZAS DE
ALGORITMOS CRIPTOGRAFICOS**

PRESENTA

Danny Ronalds Quispe Ajrota

PROFESOR

ING. Fred Torres Cruz

ASIGNATURA

COMPUTACION PARALELA

12 de octubre de 2022

USO DE PROCESADORES DE TARJETAS GRÁFICAS PARA LA VALIDACIÓN DE FORTALEZAS DE ALGORITMOS CRIPTOGRAFICOS

Danny Ronalds Quispe Ajrota

Universidad Nacional del Altiplano

daquispea@est.unap.edu.pe

Puno-Perú

Resumen

Las tarjetas gráficas, históricamente han evolucionado en su arquitectura y poder de cómputo para llevar a cabo la tarea de procesar imágenes y videojuegos de una manera más fluida y con un mayor realismo, pero desde hace algún tiempo los fabricantes de estas se han desviado de ese propósito para replantearse la utilización y el enfoque de esta tecnología, y ampliar el espectro de uso de las tarjetas gráficas. ([Martín Vieites y Collado García,](#))

Por esta razón las tarjetas gráficas dejan de ser simplemente un dispositivo hardware que se emplea en computación gráfica, y pasan a ser componentes que pueden ser utilizados para ejecutar cálculos complejos provenientes de aplicaciones que trabajan sobre ellas. ([Ruiz Velasco Sánchez,](#))

Es así como estas se vuelven más programables y permiten que los desarrolladores de aplicaciones de diferentes áreas puedan emplearlas para codificar algoritmos que las utilicen para llevar a cabo cálculos de gran envergadura debido a su gran potencia y velocidad de cómputo. ([Fernández-Herrera,](#))

El nuevo enfoque de las tarjetas gráficas, ha impulsado el desarrollo de diferentes lenguajes y entornos de programación que faciliten al desarrollador de aplicaciones la codificación de algoritmos que puedan funcionar sobre ellas. Es así como en el presente existe un entorno de programación llamado CUDA, el cual posee variadas características, dentro de las más destacables se encuentran su propio modelo de programación y la capacidad de utilizar el lenguaje de programación C como un lenguaje de alto nivel añadiéndole un conjunto de extensiones para que pueda soportar la programación de las tarjetas gráficas. ([Morillo, Fernández, y Arnau,](#))

Como en todo proyecto, es importante ir conociendo poco a poco las aristas de este. Es por esto que se identifica el origen del tema y la definición, a grandes rasgos. Se hace un resumen de la historia de las tarjetas gráficas y como estas han evolucionado en el tiempo. Se presenta los lenguajes de programación para tarjetas gráficas clasificados como GPGPU, y para concluir el estado del arte, también veremos algunos proyectos exitosos desarrollados con la tecnología. ([Echevarría,](#))



Figura 1: Evolución de las tarjetas graficas

Referencias

- Echevarría, J. (2008). Tarjetas gráficas para acelerar el cómputo complejo. *Ciencia y tecnología*, 8, 45–51.
- Fernández-Herrera, D. G. (2014). *Implementación basada en co-simulación hw de un algoritmo criptográfico en una fpga*. (Tesis de Master no publicada).
- Martín Vieites, N., y Collado García, J. (2014). Explotación de aceleradores y hardware gráfico de forma amigable.
- Morillo, P., Fernández, M., y Arnau, V. (s.f.). *Unas primeras aproximaciones evolutivas al problema del particionado en mundos virtuales distribuidos*. MAEB.
- Ruiz Velasco Sánchez, E. (2007). *Educatrónica: innovación en el aprendizaje de las ciencias y la tecnología*. Ediciones Díaz de Santos.