
# OPTIMIZACION DEL SISTEMA DE CIFRADO CSAC MEDIANTE PARALELIZACION Y ARQUITECTURAS DE HARDWARE ESPECIALIZADAS.

Jesus Agustin Aboytes Gonzalez[1], Marcela Mejía Carlos[1] y José Salomé Murguía Ibarra[2]

1 Instituto de Investigación en Comunicación Óptica, Universidad Autónoma de SLP, 2 Facultad de Ciencias de la Universidad Autónoma de SLP.. j.a.a.g.85@hotmail.com

El objetivo de este trabajo es la optimización del sistema de cifrado CSAC (Cifrado por Sincronización de Autómatas Celulares), debido al gran número de operaciones que se necesitan realizar para cifrar o descifrar un bloque de información por lo que las aplicaciones en tiempo real no pueden ejecutarse correctamente. Lo anterior se realizó mediante la implementación de técnicas de paralelización y el uso de arquitecturas de hardware especializadas, como lo son los GPU's y los FPGA's. Debido a que en el sistema CSAC existe una dependencia de información cuando se procesa un bloque de datos no se puede paralelizar completamente, con lo que se recurren a técnicas de pseudo paralelismo como lo son el pipeline. Los resultados obtenidos fueron satisfactorios ya que se disminuyeron los tiempos de ejecución hasta en 60%, con lo cual se logro un mejor desempeño en la ejecución de aplicaciones en tiempo real.
Agradecimiento: CONACyT.