Seminario de Investigación

Curso 2015-16

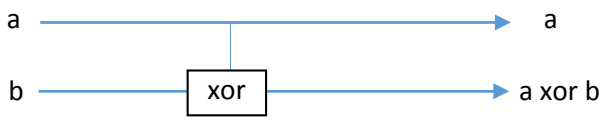
Martes 15 de marzo, 16:00 - Sala de Grados. Conferencia:

"Investigación en Computación Reversible"

Ponente: *Jesús García López de Lacalle, profesor de la UPM*

Resumen:

Decimos que un circuito lógico es reversible si se puede ejecutar hacia atrás. Por ejemplo, el circuito 1 es reversible y el 2 no:



Circuito 1

Circuito 2

Decimos que la computación es reversible si se realiza mediante circuitos lógicos reversibles. Este tipo de computación es objeto de investigación actualmente por dos razones fundamentalmente:

1. *Permite optimizar más el consumo de energía.*
2. *Permite abordar la ruptura de sistemas criptográficos de clave pública basados en funciones de dirección única (one way functions), tales como el producto (función inversa: factorización) o la exponencial discreta (función inversa: logaritmo discreto) de números naturales.*

En la charla vamos a introducir la computación reversible y vamos a plantear como PFM la definición de un lenguaje de alto nivel para programación reversible.