



POLITÉCNICA



Universidad
Politécnica
de Madrid

ETSI SISTEMAS
INFORMÁTICOS

Máster en Ciencias y Tecnologías de la Computación

Propuesta de tema para Trabajo Fin de Máster

Curso 2015-16

Título: Computación reversible. Aplicación a *one-way functions*

Directores: Jesús García López de Lacalle

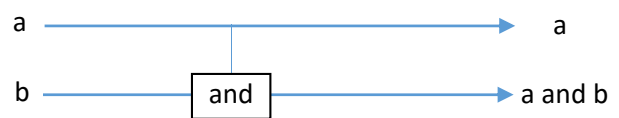
¿Es un tema de tesis doctoral? Sí ☐ NO ☒

Resumen

Decimos que un circuito lógico es reversible si se puede ejecutar hacia atrás. Por ejemplo, el circuito 1 es reversible mientras que el 2 no lo es. Decimos que la computación es reversible si se realiza mediante circuitos lógicos reversibles.



Circuito 1



Circuito 2

El objetivo de este trabajo es definir un conjunto universal de puertas lógicas reversibles, que permitan la construcción de circuitos lógicos reversibles, para aplicarlo al cálculo de las inversas de algunas one way functions, por ejemplo, la multiplicación de números naturales. Estos resultados nos permitirán realizar criptoanálisis de sistemas criptográficos basados en dichas one way functions.