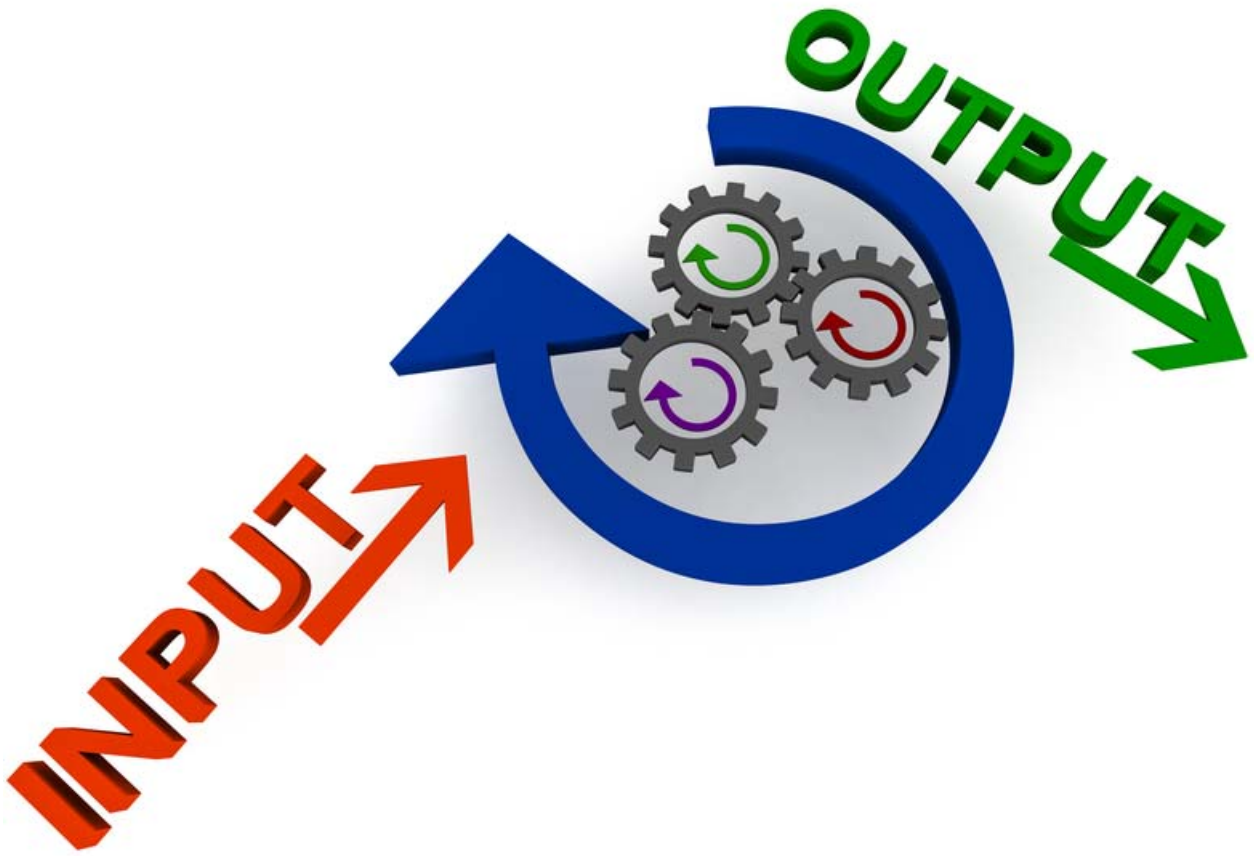
Máster en Ciencias y Tecnologías de la Computación

Seminario de Investigación

# Investigación en Computación Reversible

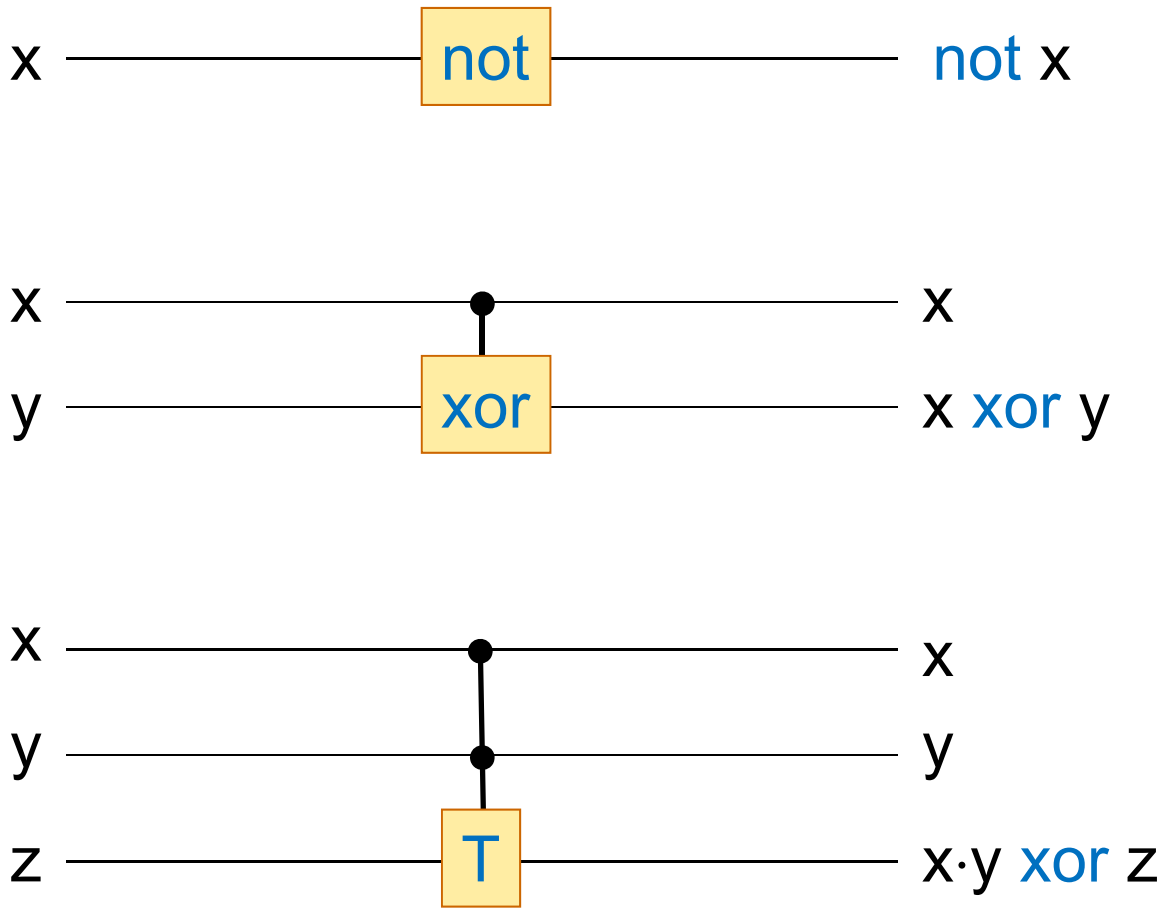
Jesús García

15 de marzo de 2016



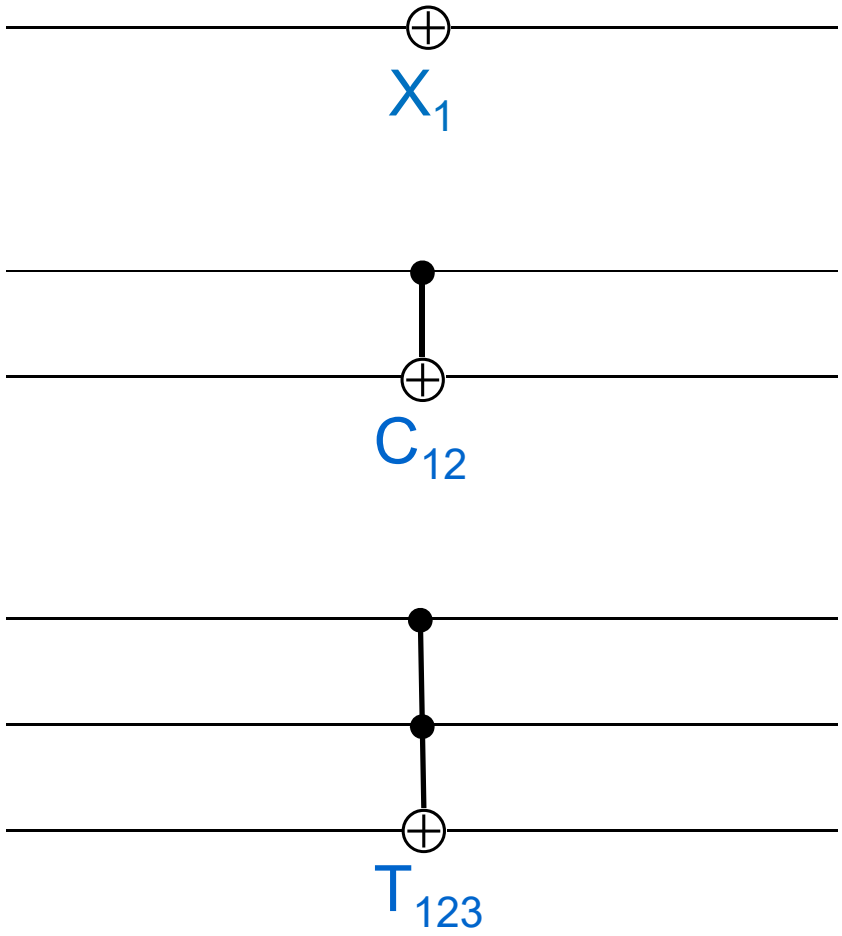

## Computación Reversible:

- Input → Output
- Output → Input



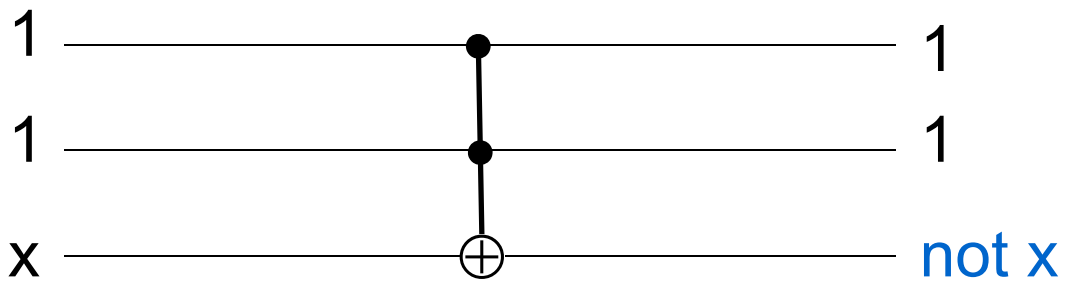

## Puertas lógicas reversibles:

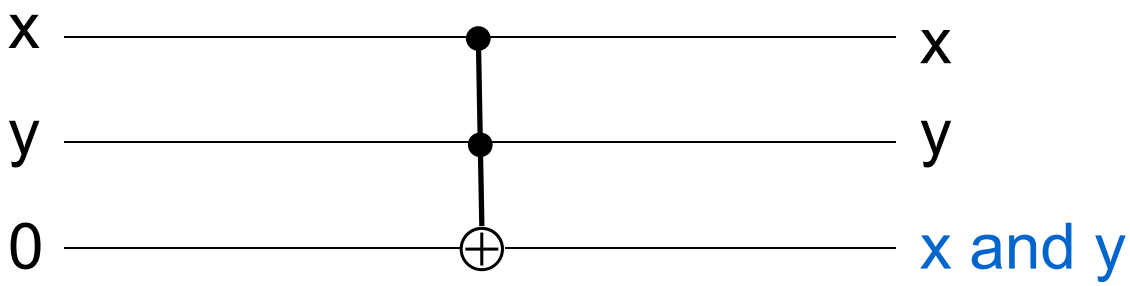
- not → X (negación)
  - X(0) = 1
  - X(1) = 0
- xor → C (negación controlada)
  - C(00) = 00
  - C(01) = 01
  - C(10) = 11
  - C(11) = 10
- T (Toffoli – negación bicontrolada)
  - T(000) = 000
  - T(001) = 001
  - T(010) = 010
  - T(011) = 011
  - T(100) = 100
  - T(101) = 101
  - T(110) = 111
  - T(111) = 110




## Puertas lógicas reversibles:

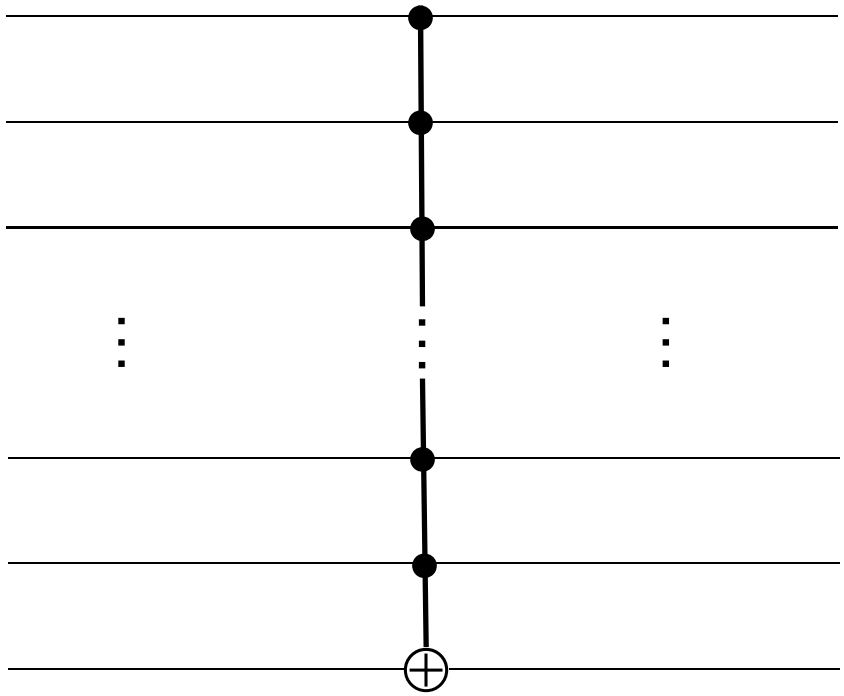
- Notación



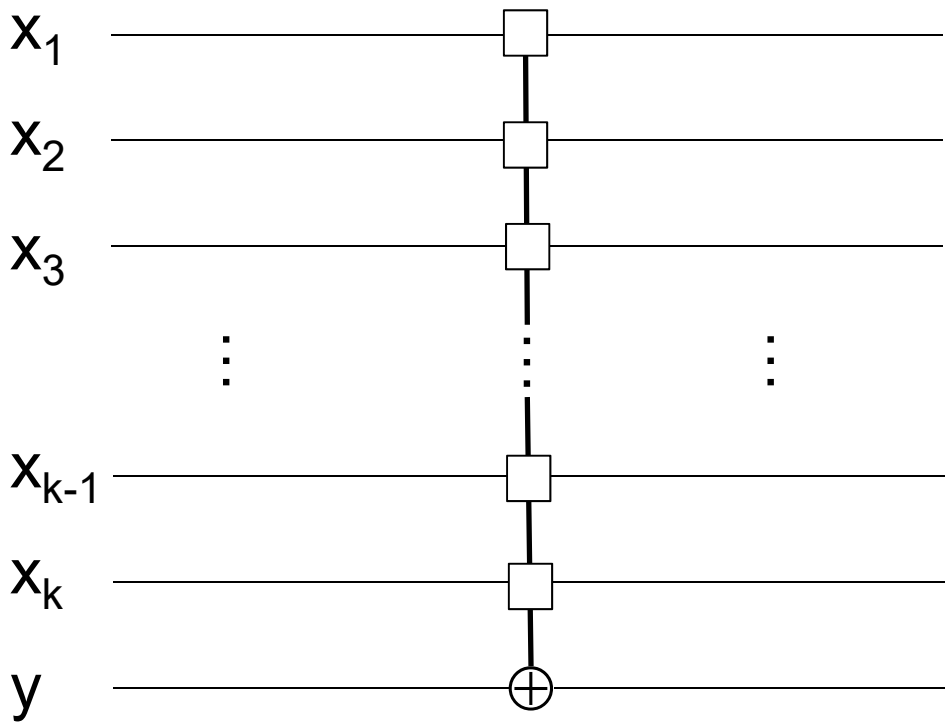

Puertas lógicas reversibles:

- Notación
- Universalidad de T



## Puertas lógicas reversibles:

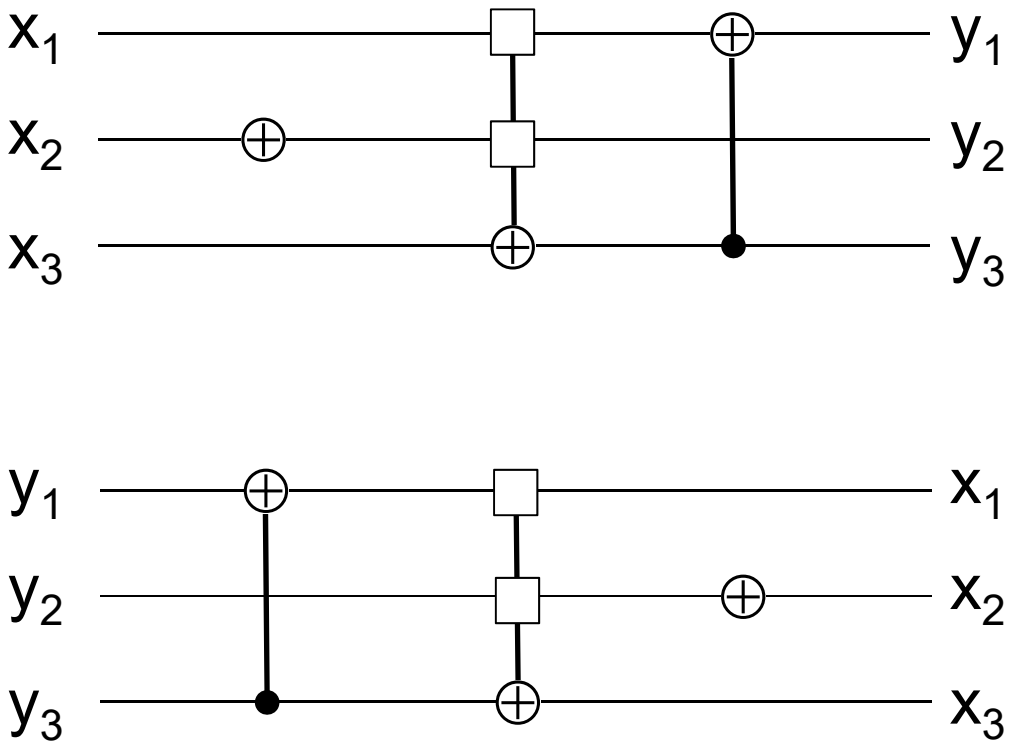
- Notación
- Universalidad de T
- Puerta T generalizada




## Puertas lógicas reversibles:

- Notación
- Universalidad de T
- Puerta T generalizada
- Puerta T universal

Se aplica la negación a y si se verifica $f(x_1, \ldots, x_k) = 1$



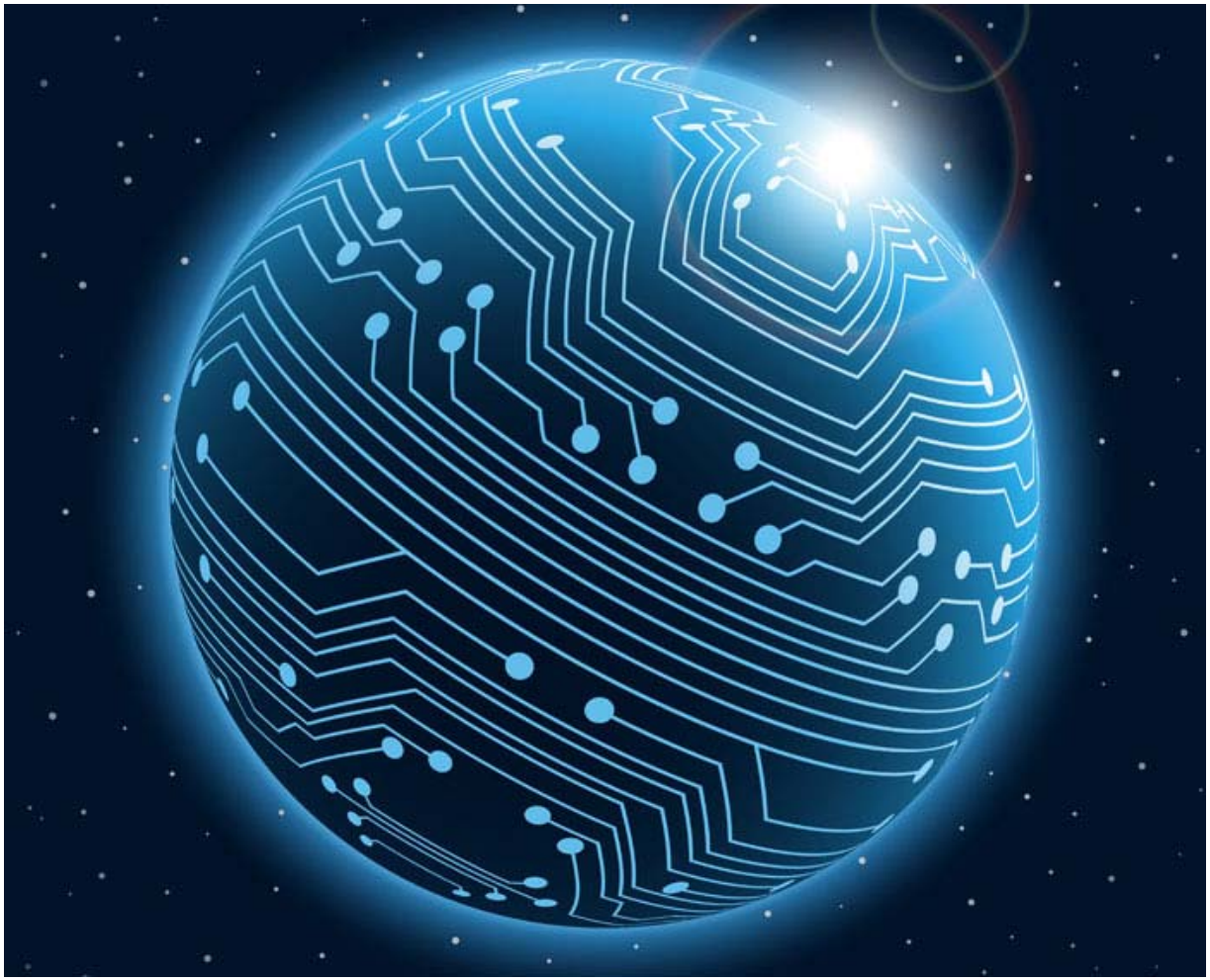

## Invertir un algoritmo:

- Poner las puertas lógicas en orden inverso
- Sustituir cada puerta por su inversa

Las puertas X, C, T, T-generalizada y T-universal son autoinversas

Máster en Ciencias y Tecnologías de la Computación

Seminario de Investigación



## Objetivos:

- Ahorro energético
- Algorítmica

## Objetivos:

- Ahorro energético

**World energy use per sector**

| Year | 2000 | 2008 | 2000 | 2008 |
|---|---|---|---|---|
| **Sector** | **TWh** | | **%*** | |
| Industry | 21,733 | 27,273 | 26.5 | 27.8 |
| Transport | 22,563 | 26,742 | 27.5 | 27.3 |
| Residential and service | 30,555 | 35,319 | 37.3 | 36.0 |
| Non-energy use | 7,119 | 8,688 | 8.7 | 8.9 |
| **Total*** | **81,970** | **98,022** | **100** | **100** |

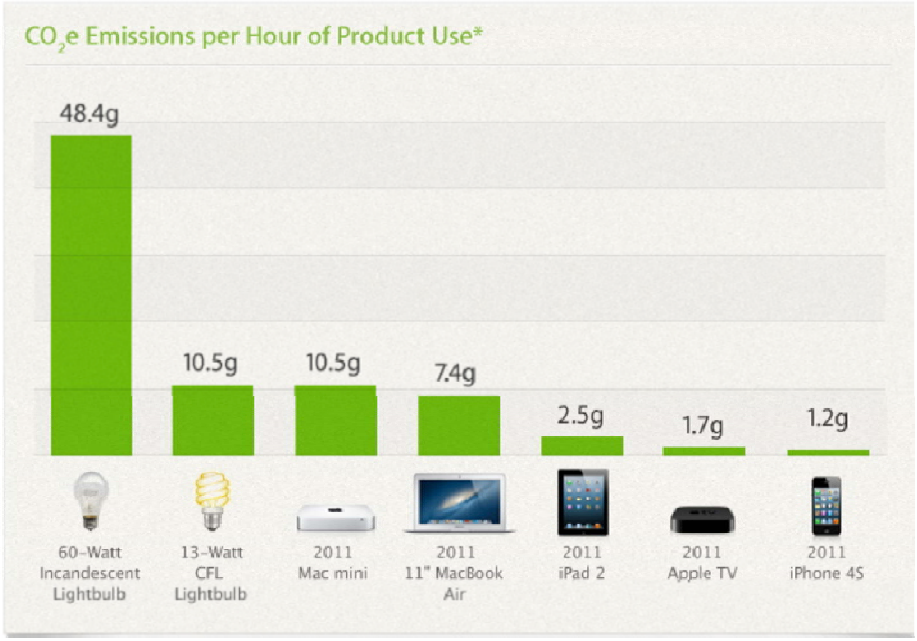
Source: IEA 2010, Total is calculated from the given sectors
Numbers are the end use of energy
Total world energy supply (2008) 143,851 TWh

Máster en Ciencias y Tecnologías de la Computación

Seminario de Investigación

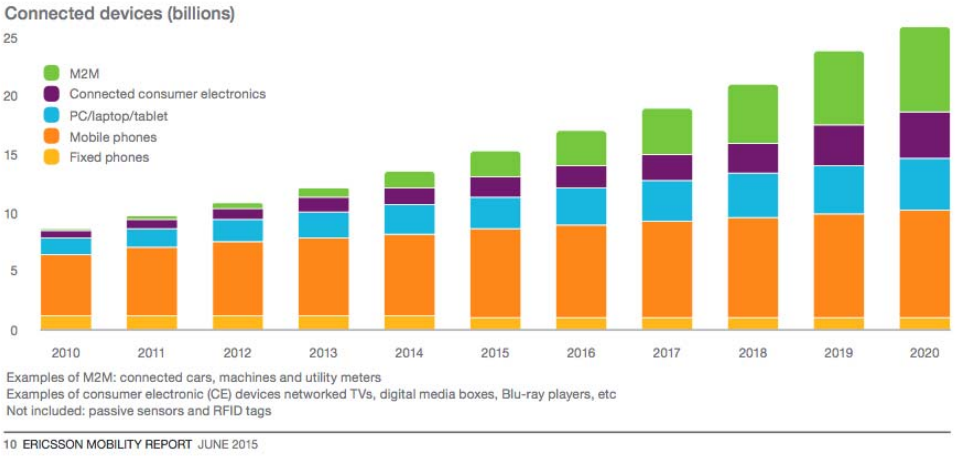
## Objetivos:

- Ahorro energético



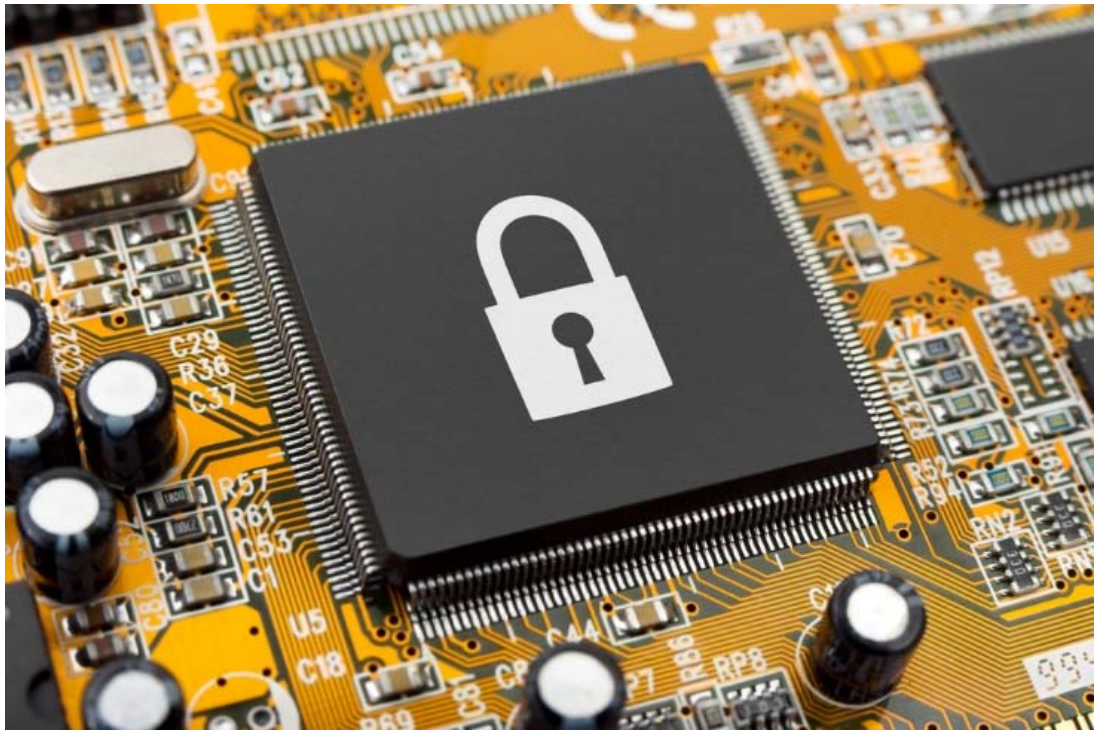
## Objetivos:

- Ahorro energético
- La computación reversible permite un mayor ahorro energético



## Objetivos:

- Algoritmos
- Aplicaciones en:
  Ingeniería Informática
  Ciencias
  Medicina
  Economía
  Criptografía



## Criptografía:

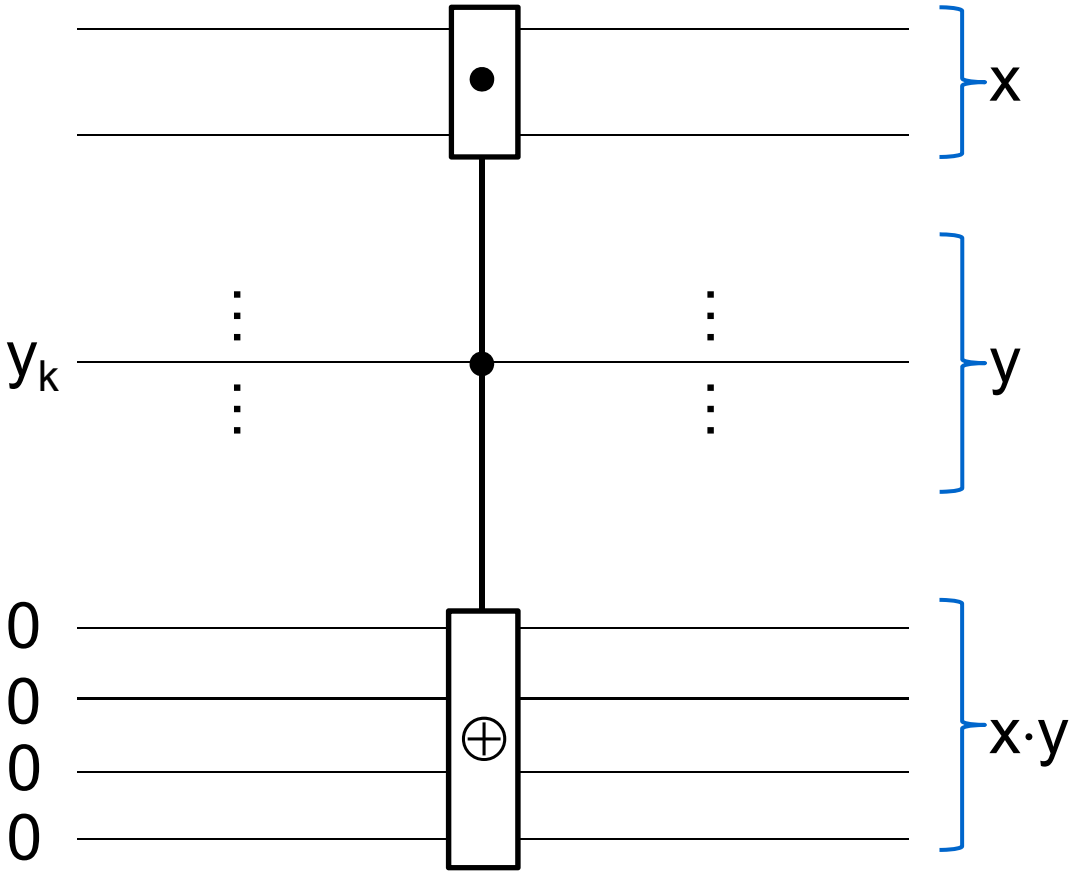
- One-way functions:
- Multiplicación
  Cuadrado modular
  Exponenciación modular
  Curvas elípticas
  Códigos lineales

## Multiplicación

- Estrategia

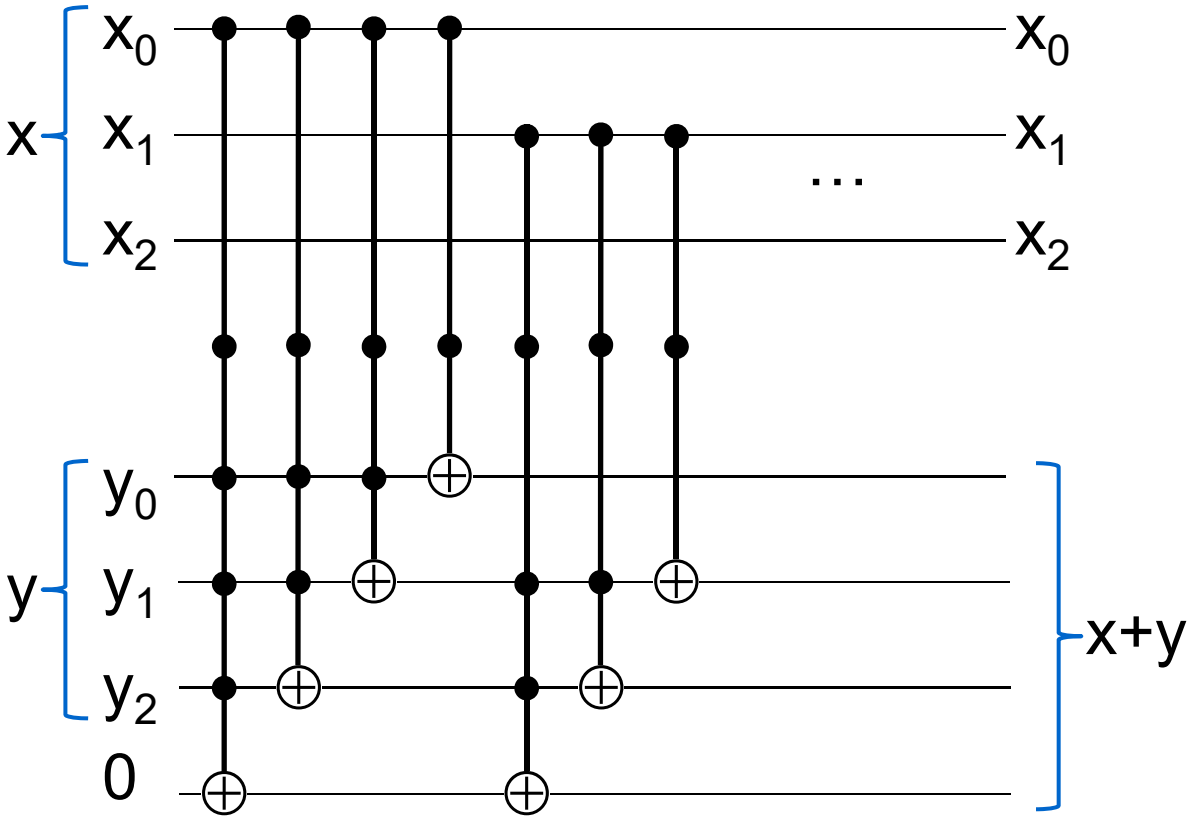
**BINARY MULTIPLICATION**

```
      1101    (13)
    x 1011    (11)
  ------
      1011
     0000
+   1011
   1011
  ------
  10001111    (143)
```




## Multiplicación

- Estrategia
- Para todo k sumamos x, si $y_k = 1$, en el registro producto, a partir del bit k




## Multiplicación

- Suma
- Para todo k sumamos $x_k$
- Empezamos por los acarreos
- 1+ 111 → acarreo en $y_3$
- 1+ ·11 → acarreo en $y_2$
- 1+ ··1 → acarreo en $y_1$
- Suma de $x_0$ en $y_0$


## Multiplicación

- Borrado:
- Permite calcular la inversa, por tanto, factorizar
- No se puede hacer un borrado completo
- Objetivo:
- Borrar todo a excepción de O(poy(log(n))) bits, siendo n el máximo número de bits de x e y


Máster en Ciencias y Tecnologías de la Computación

Seminario de Investigación


# Computación reversible. Aplicación a one-way functions

Proyecto Fin de Máster

# Preguntas…