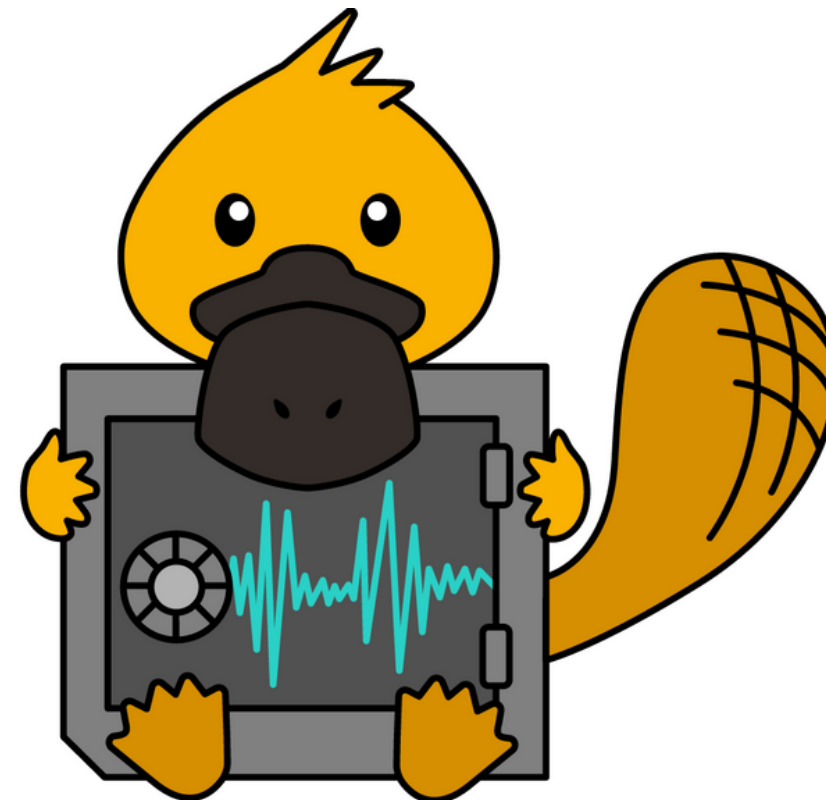


Universidad  
Industrial de  
Santander

# PLUNDERVOLT AND PLATYPUS

---



Andrés Felipe Perez 2170499  
Luis Alejandro Hernández Ríos 2171773



plunder: 'plən-dər To steal or remove something precious from something, in a way that does not consider moral laws.

# PLUNDERVOLT

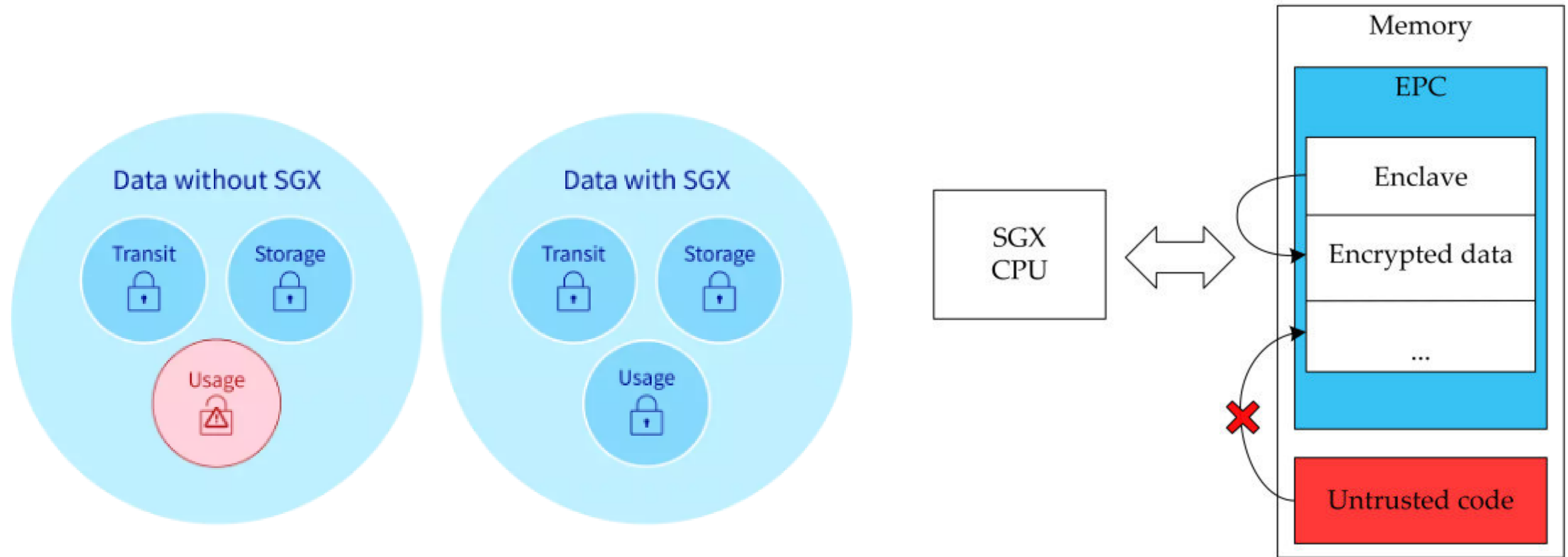
---

Reportado por primera vez el 7-junio-2019 por:

- Kit Murdock, David Oswald, Flavio D Garcia (The University of Birmingham)
- Jo Van Bulck, Frank Piessens (imec-DistriNet, KU Leuven)
- Daniel Gruss (Graz University of Technology)

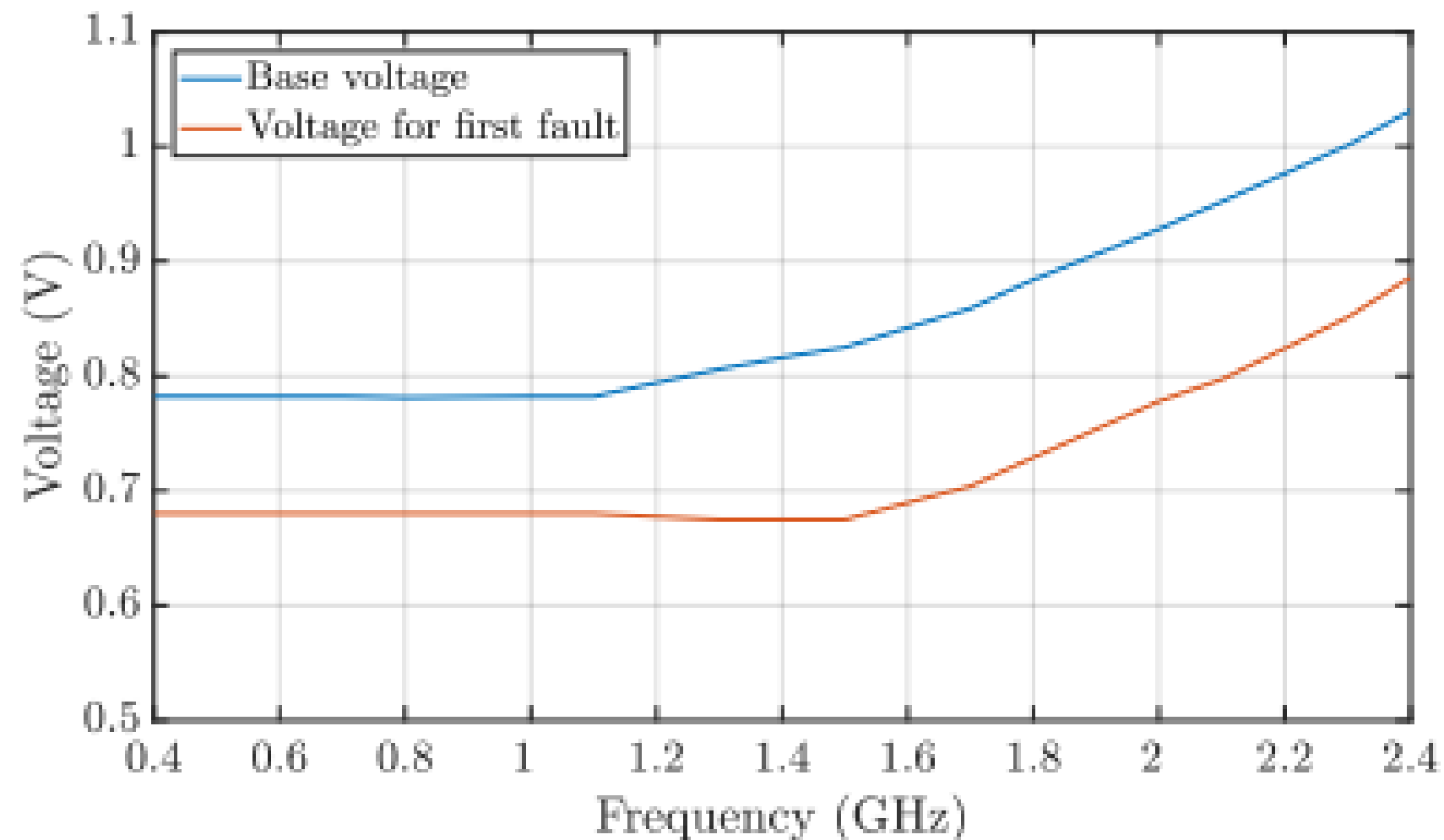
# Intel SGX

## Intel software Guard extensions (SGX)



# Implicaciones

- Falla en las multiplicaciones emitidas por el compilador para índices de elementos de matriz o aritmética de punteros.



NUMBER OF ITERATIONS UNTIL A FAULT OCCURS FOR THE MULTIPLICATION ( $0x\text{AE}0000 * 0x18$ ) VS. NECESSARY UNDERVOLTING ON i3-7100U-B AT 2 GHz.

Iterations	Undervolting
1,000,000,000	-130mV
100,000,000	-131mV
10,000,000	-132mV
1,000,000	-141mV
500,000	-146mV
100,000	crash at -161mV

Base voltage (Blue) and voltage for first fault (orange) vs CPU frequency for the 17-8650U-A

# Implicaciones

---

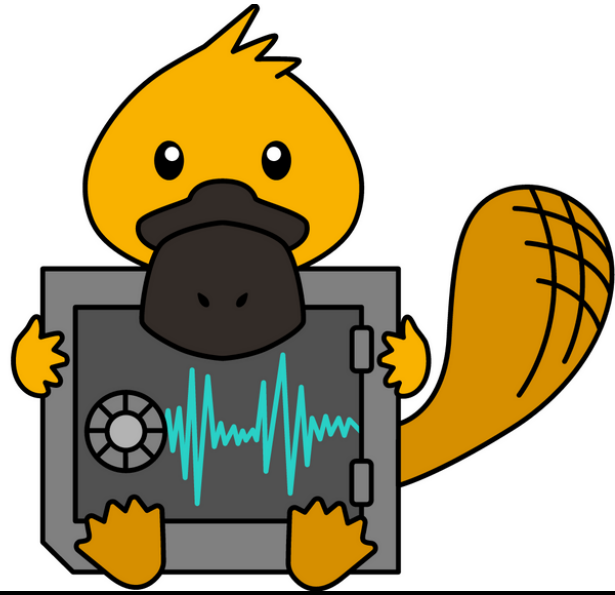
- Extracción de claves criptográficas.
- Plundervolt puede causar un comportamiento indeseado en las memorias
- Puede romper las garantías de integridad del procesador.
- Puede afectar la funcionalidad de la certificación de SGX, socavando los componentes básicos que sustentan la seguridad del mismo ecosistema SGX de Intel

# Implicaciones

---

- Extracción de claves criptográficas.
- Plundervolt puede causar un comportamiento indeseado en las memorias
- Puede romper las garantías de integridad del procesador.
- Puede afectar la funcionalidad de la certificación de SGX, socavando los componentes básicos que sustentan la seguridad del mismo ecosistema SGX de Intel

**SOLUCION**???

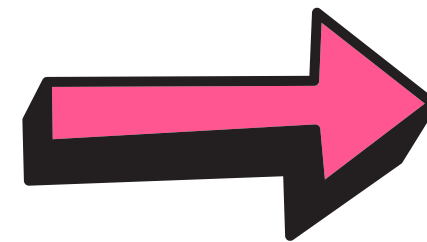


# PLATYPUS

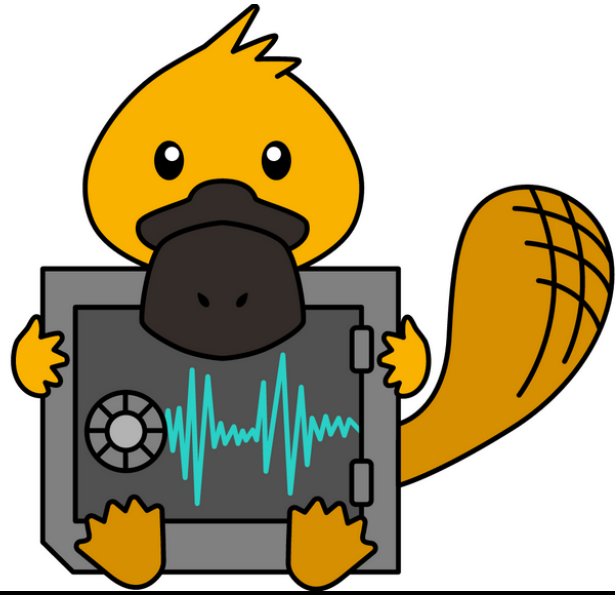
---

## Disminuir consumo de energía

- Apagar recursos
- Reducir voltaje de alimentación
- Reducir frecuencia de operación



**Intel RAPL**

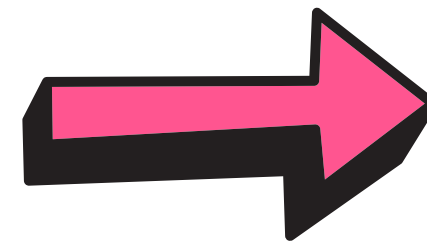


# PLATYPUS

---

## Disminuir consumo de energía

- Apagar recursos
- Reducir voltaje de alimentación
- Reducir frecuencia de operación



**Intel RAPL**

Linux:

```
/sys/devices/virtual/powercap/intel-rapl
```

Windows y MacOS :

Instalación de drivers



# Intel RAPL

---

- Medidor de energía imprivilegiado
- No se requiere acceso físico
- Tasa limitada de actualización de datos

¿Qué podemos medir?

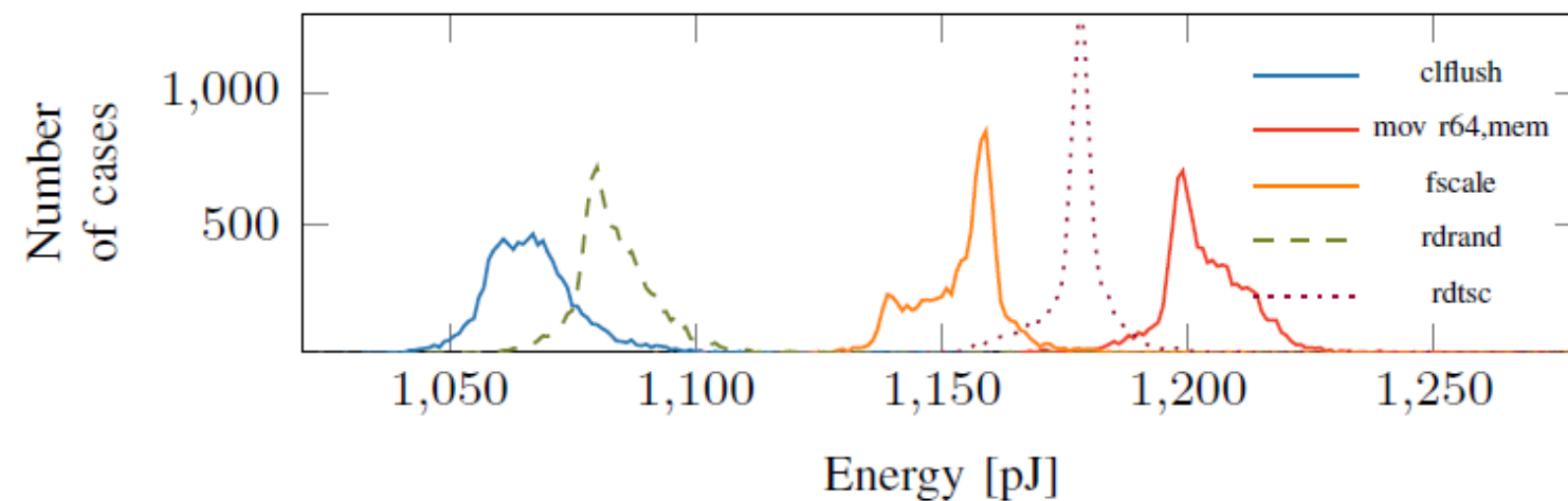
# Intel RAPL

---

- Medidor de energía imprivillegiado
- No se requiere acceso físico
- Tasa limitada de actualización de datos

## ¿Qué podemos medir?

Consumo de energía de diferentes instrucciones

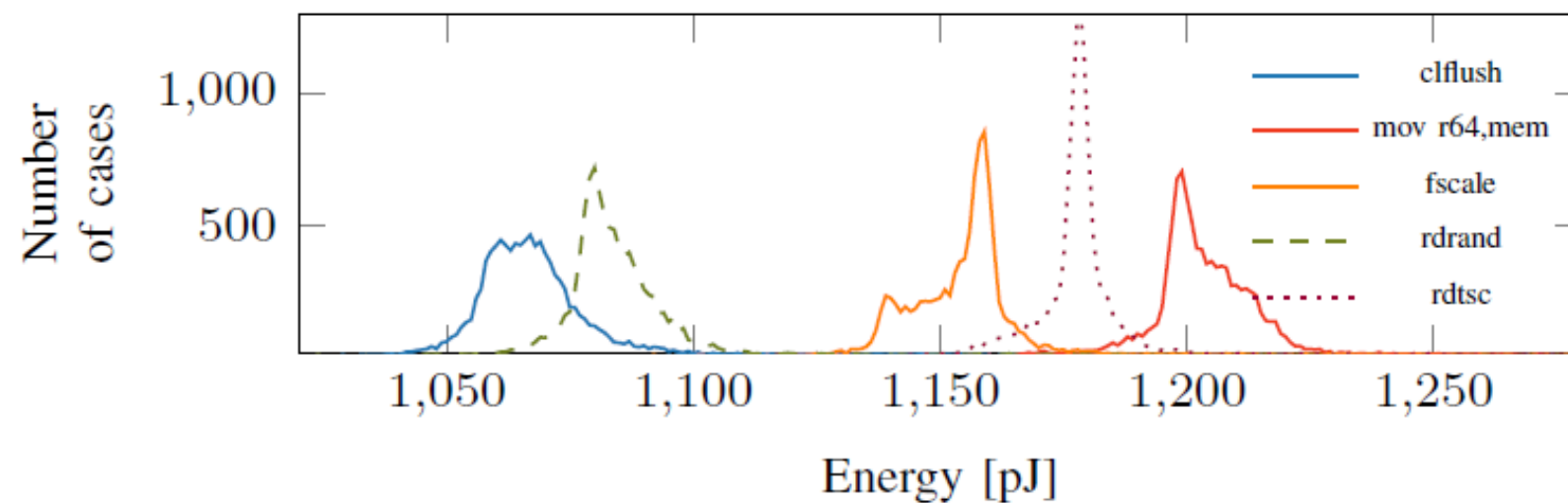


# Intel RAPL

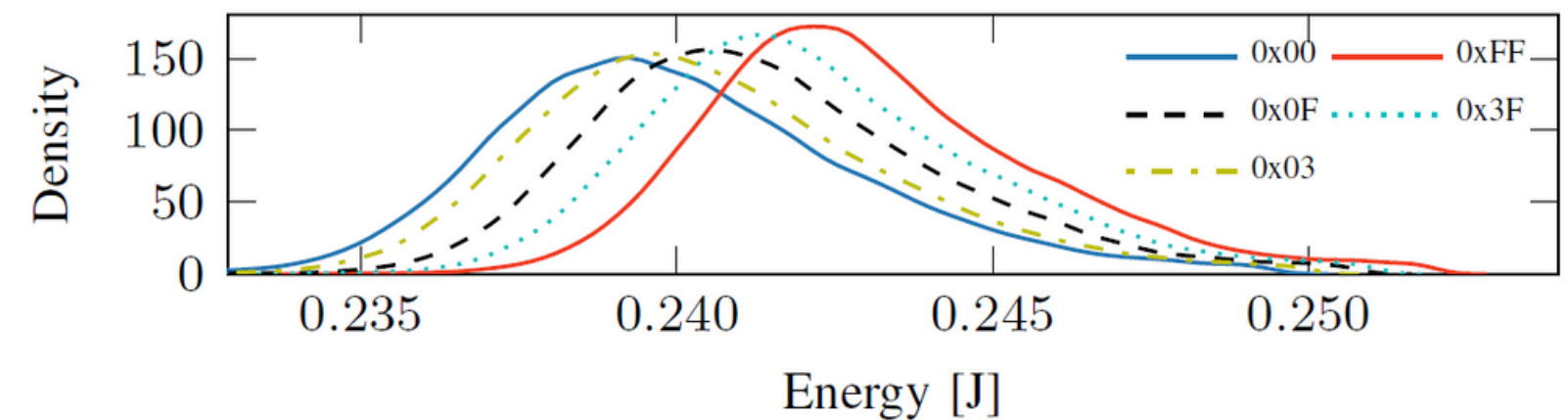
- Medidor de energía imprivillegiado
- No se requiere acceso físico
- Tasa limitada de actualización de datos

## ¿Qué podemos medir?

Consumo de energía de diferentes instrucciones



Consumo de energía de diferentes operandos



# Intel RAPL

---

- Medidor de energía imprivilegiado
- No se requiere acceso físico
- Tasa limitada de actualización de datos

## ¿Qué podemos medir?

Consumo de energía para  
diferentes valores de carga

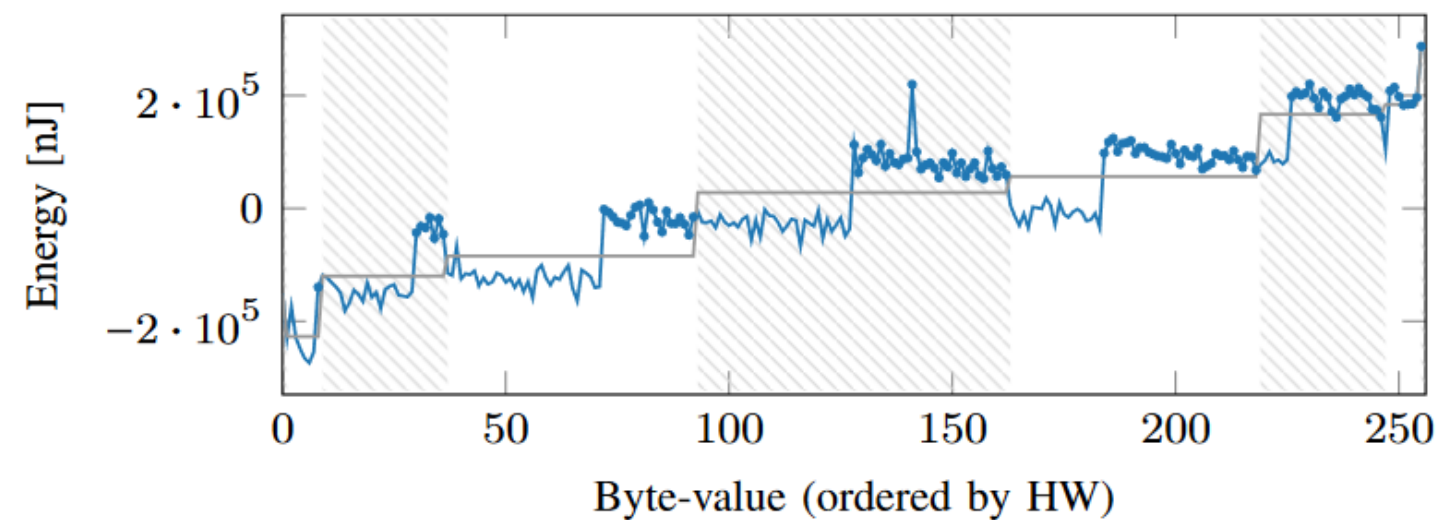
# Intel RAPL

---

- Medidor de energía imprivillegiado
- No se requiere acceso físico
- Tasa limitada de actualización de datos

## ¿Qué podemos medir?

Consumo de energía para  
diferentes valores de carga



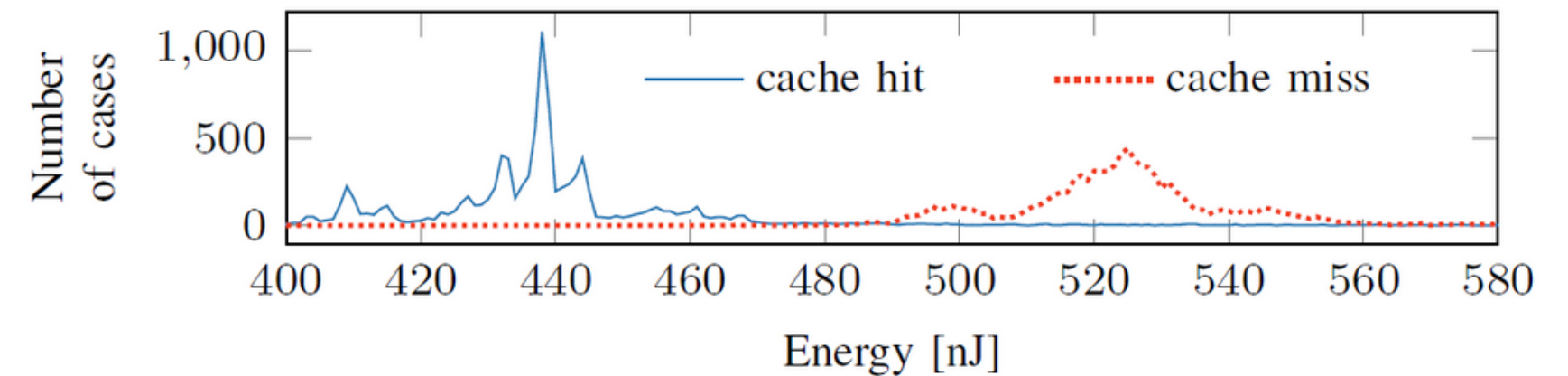
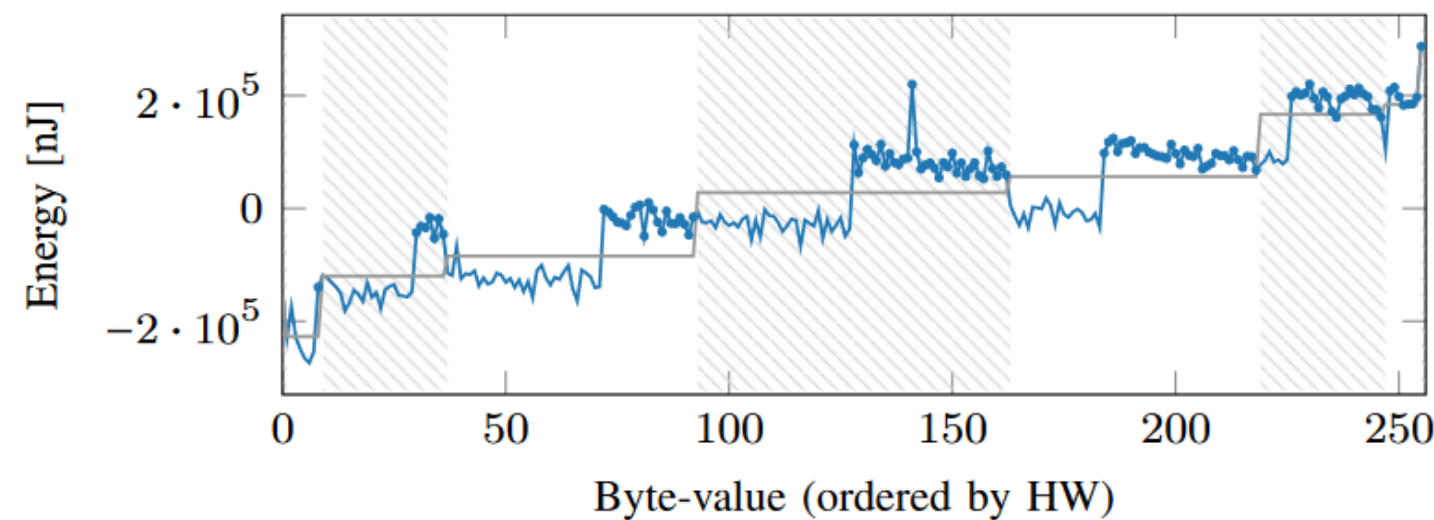
# Intel RAPL

---

- Medidor de energía imprivillegiado
- No se requiere acceso físico
- Tasa limitada de actualización de datos

## ¿Qué podemos medir?

Consumo de energía para  
diferentes valores de carga



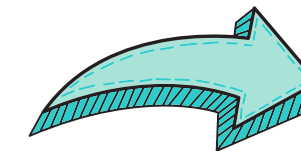
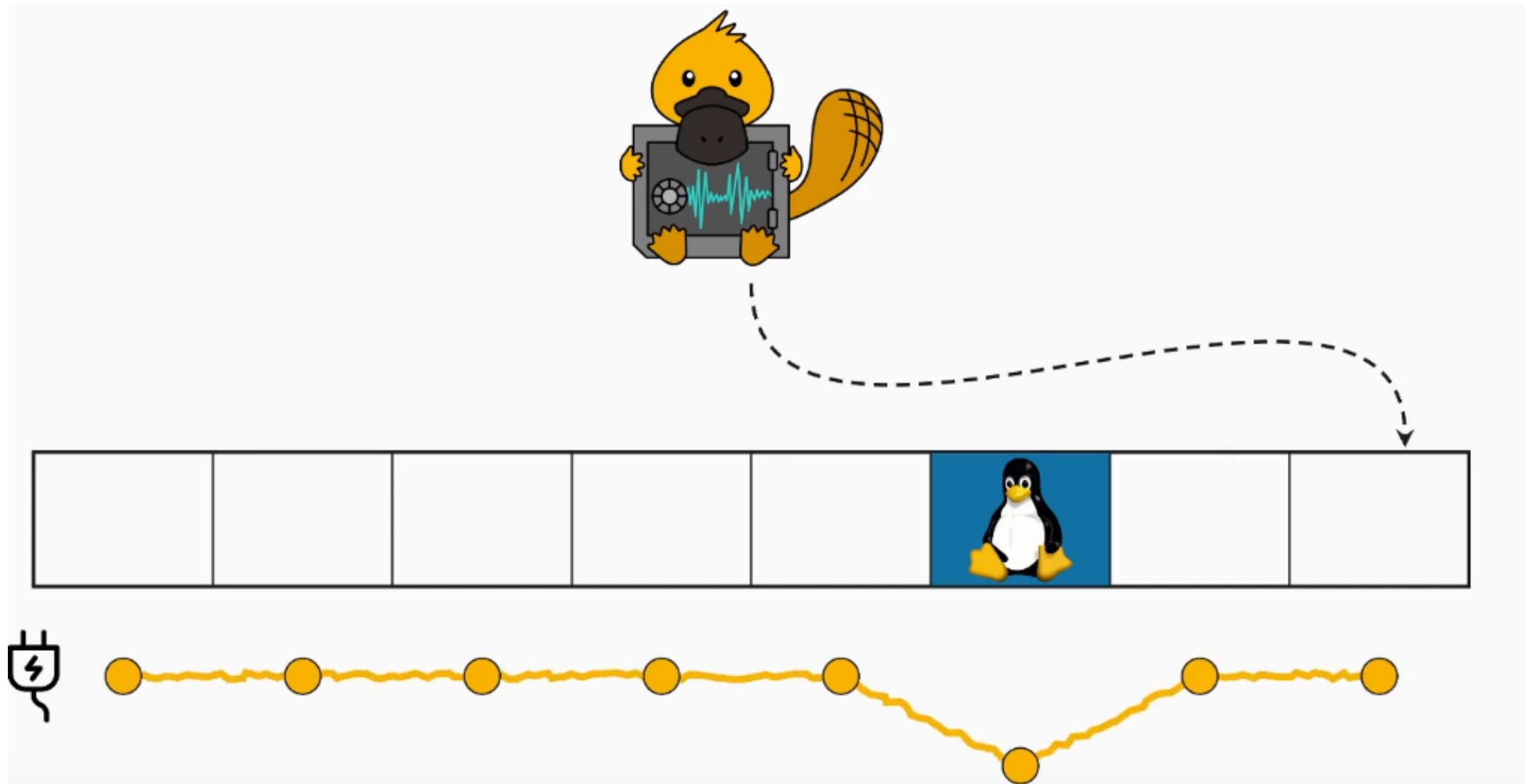
# Implicaciones

---

# Implicaciones

---

- Ataque al KASLR

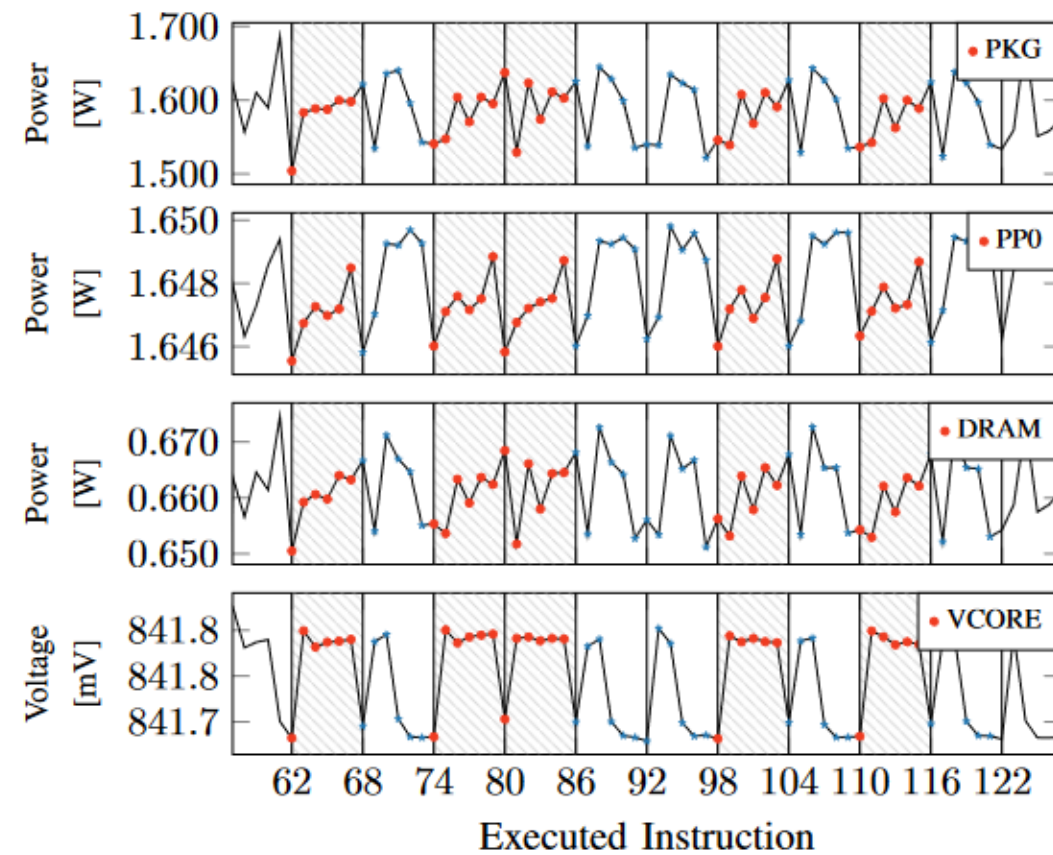


Cuando ocurre una table walk se tiene un mayor consumo de energía

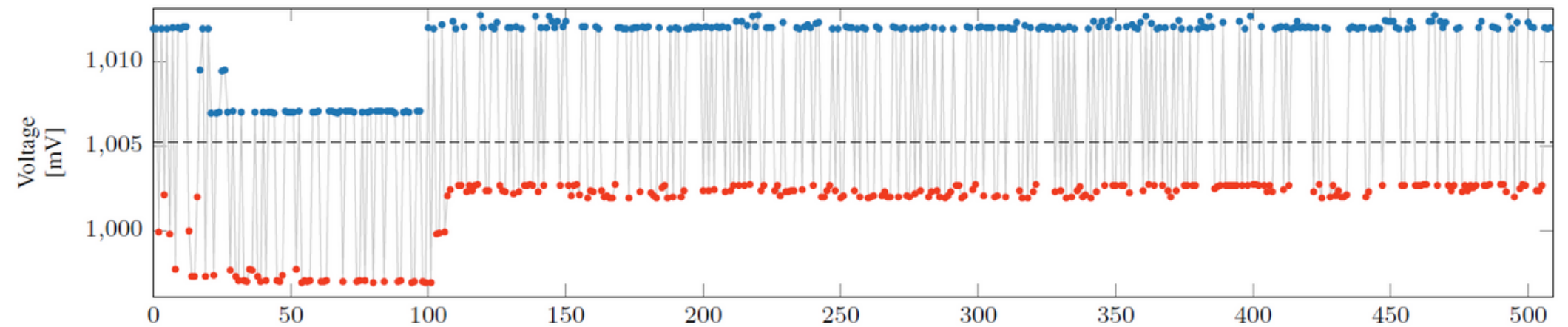


# Implicaciones

- Intel RAPLG con Intel SGX



Se puede diferenciar el 1 del cero



Eventualmente se puede obtener la ARS key completa

# CounterMeasures

---

# CounterMeasures

---



- Remover el acceso no privilegiado a RAPL



**RAPL**

# CounterMeasures

---

- Remover el acceso no privilegiado a RAPL  **RAPL**
- Cambiar el modelo de medición de energía  **Intel SGX**

# CounterMeasures

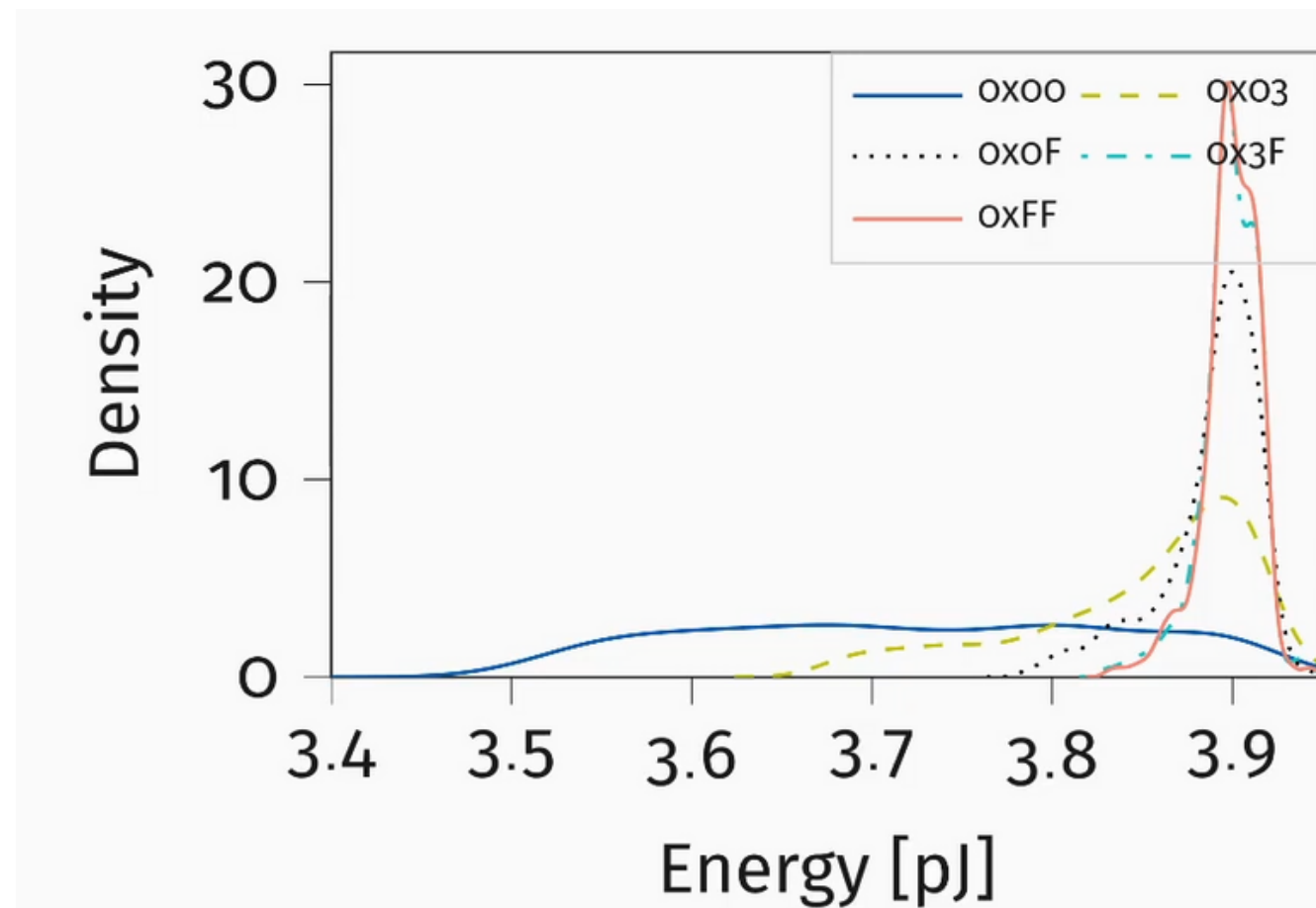
- Remover el acceso no privilegiado a RAPL
- Cambiar el modelo de medición de energía



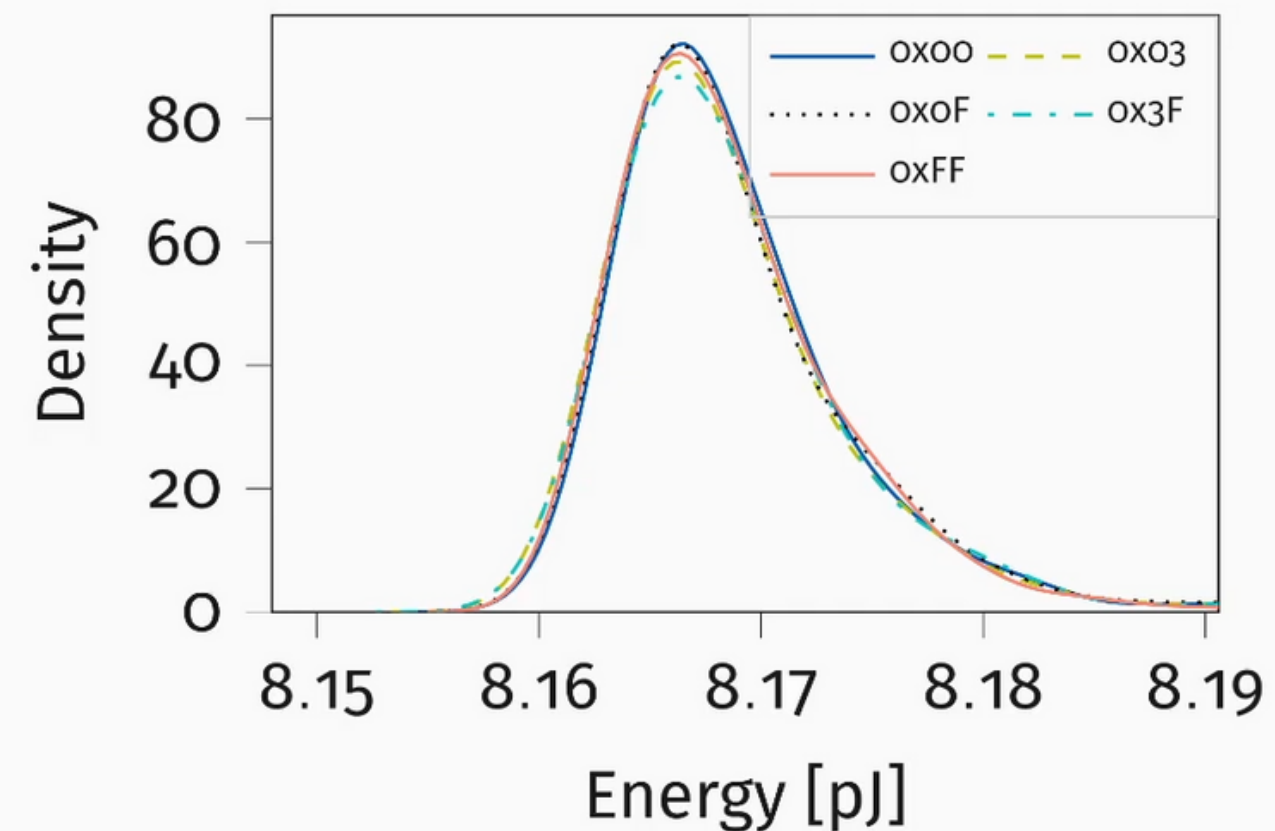
**RAPL**



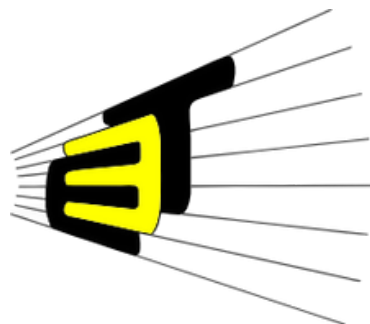
**Intel SGX**



Sin mitigación



Con mitigación



*¡Gracias!*