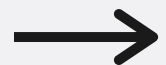




PROPUESTA DE MEJORA - SNOW VI



PARADIGMA ACTUAL



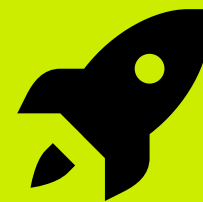
2
→



Requisitos básicos del 3GPP

256

Claves de 256 bits



Mínimo 20Gbps / 100Gbps



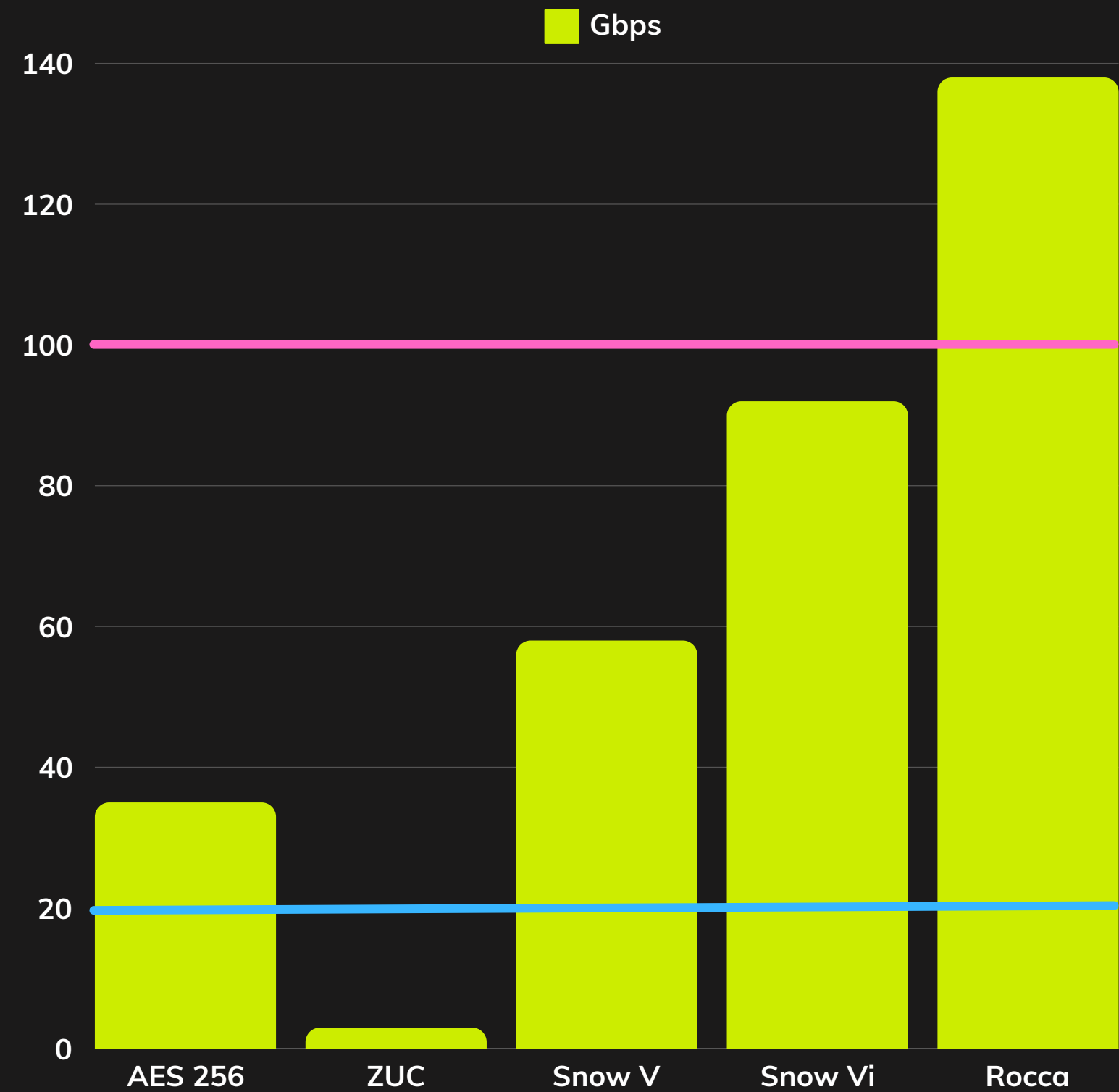
Entornos virtualizados

3



VELOCIDADES

Comparativa de velocidades estimadas



SNOW-VI

Estructura

LFSR

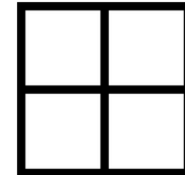
Linear Feedback Shift Register

FSM

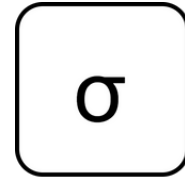
Finite State Machine



FSM



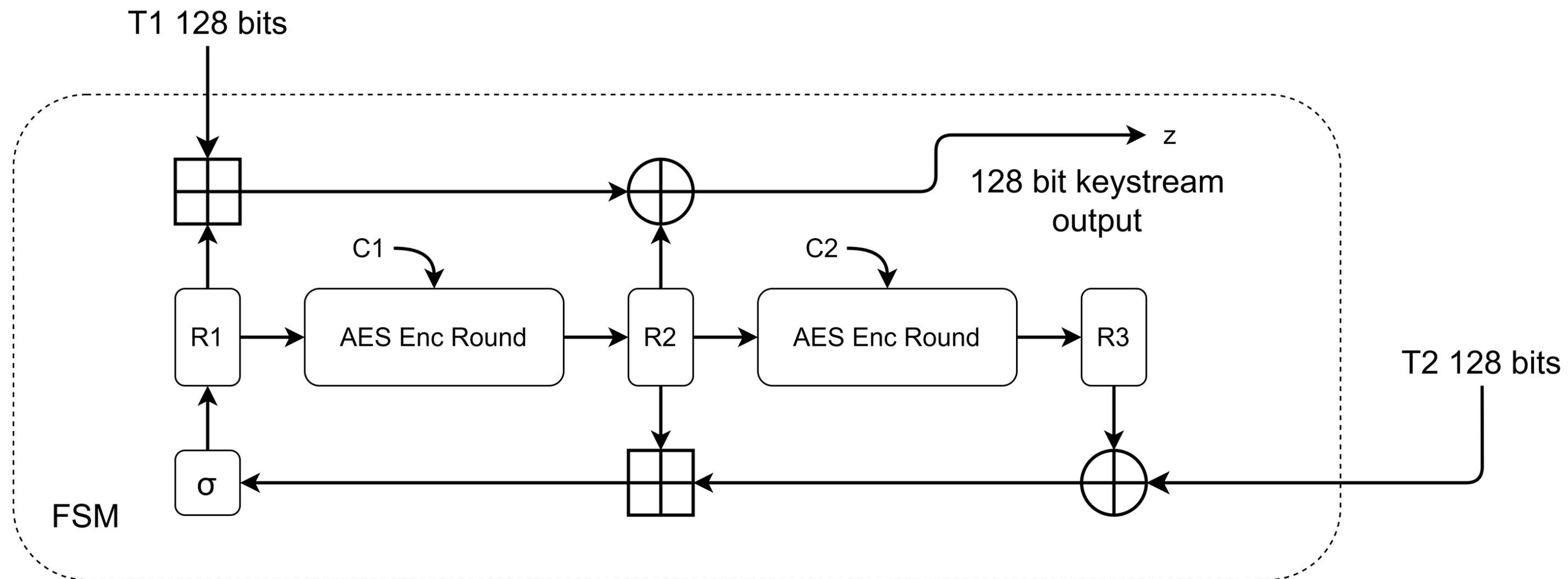
4 sumas paralelas en módulo 2^{32}



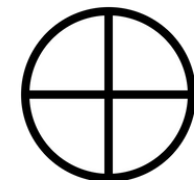
Desplazamiento de bits siguiendo

Sigma:

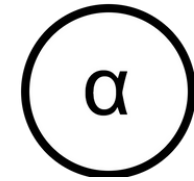
[0, 4, 8, 12, 1, 5, 9, 13, 2, 6, 10, 14, 3, 7, 11, 15]



LFSR

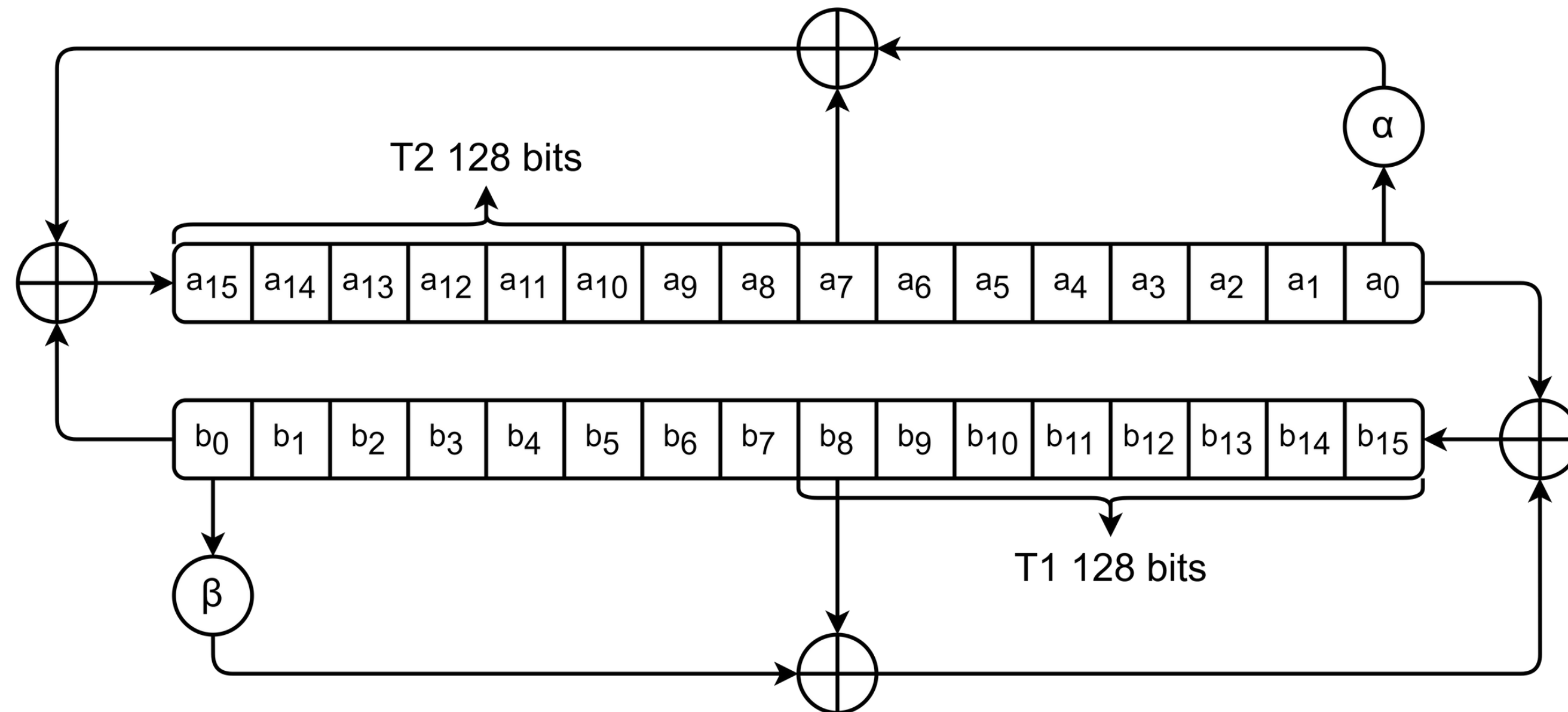


Operación XOR



Multiplicación por α

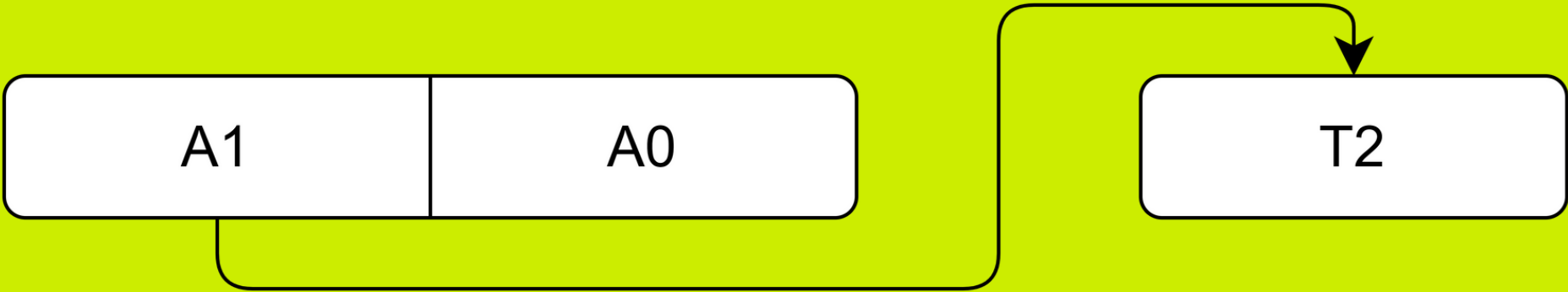
Ciclo: $2^{512} - 1$



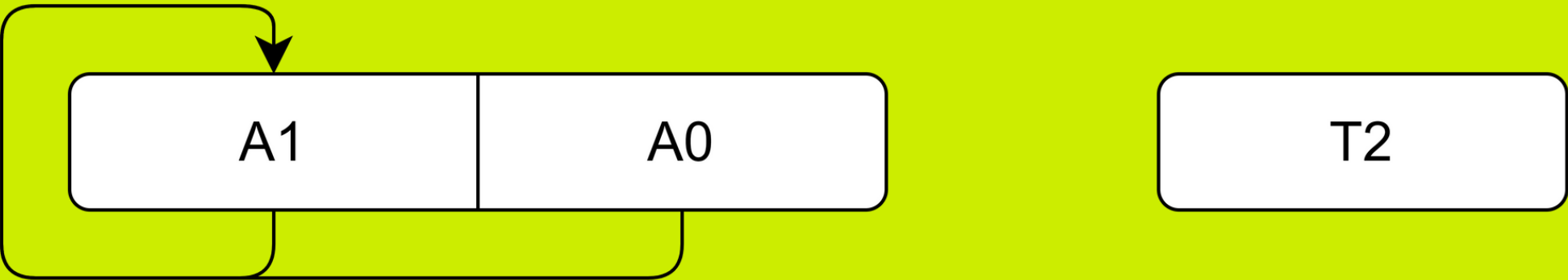
7
→

SNOW-VI

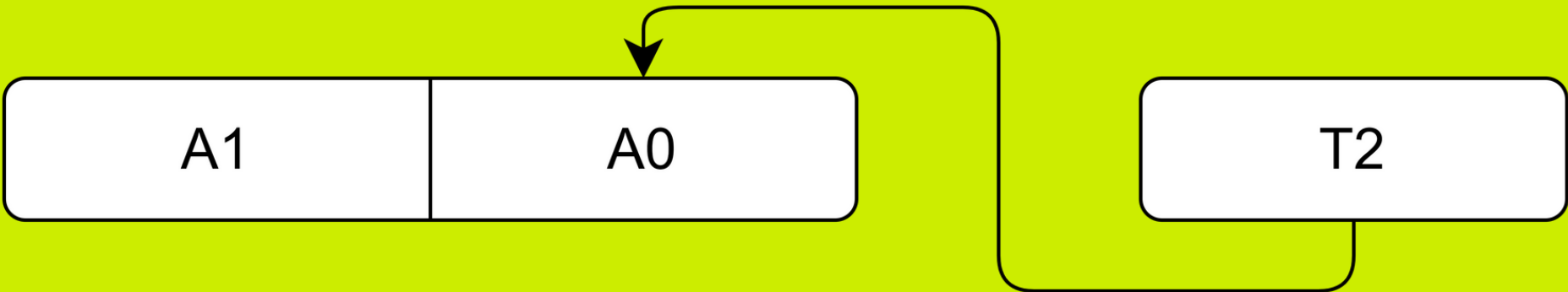
P1



P2

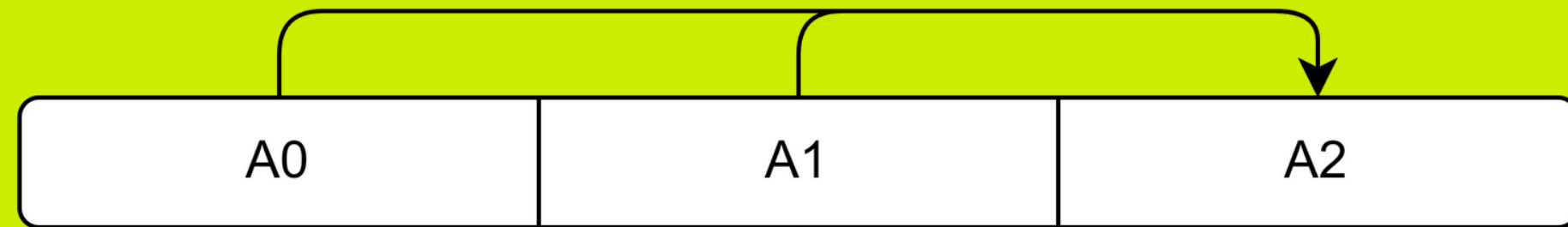


P3

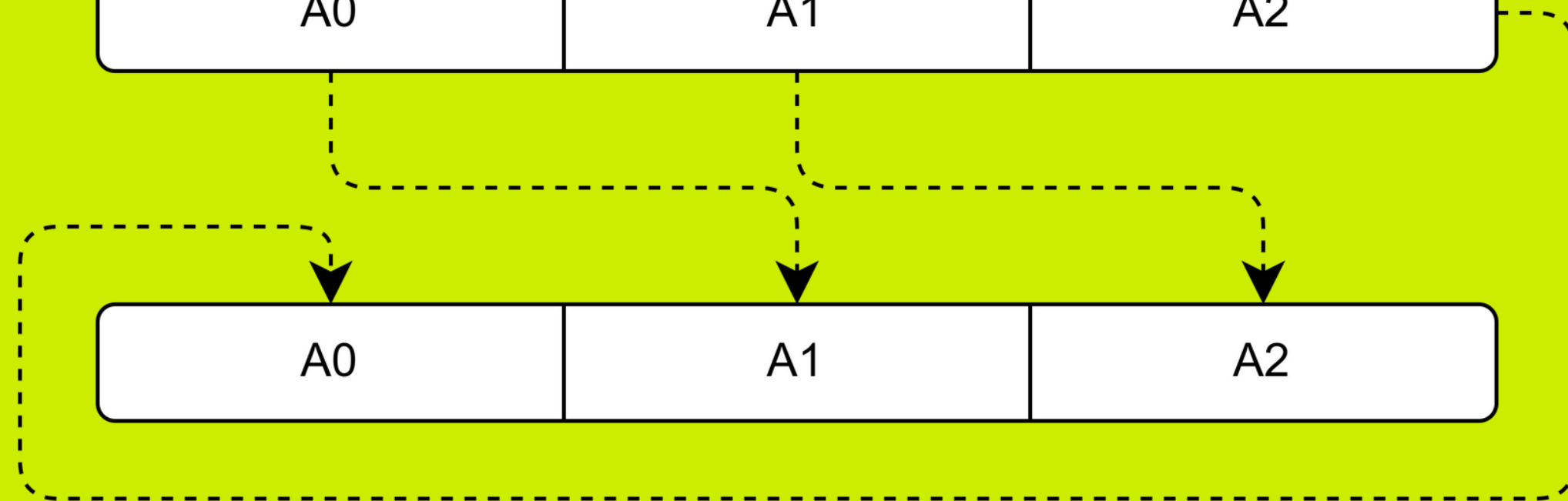


PROPUESTA

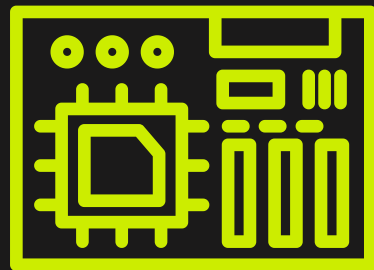
P1



P2



Tipos de dispositivos



SBC
ARM



Ordenadores
x86



WorkStation
x86

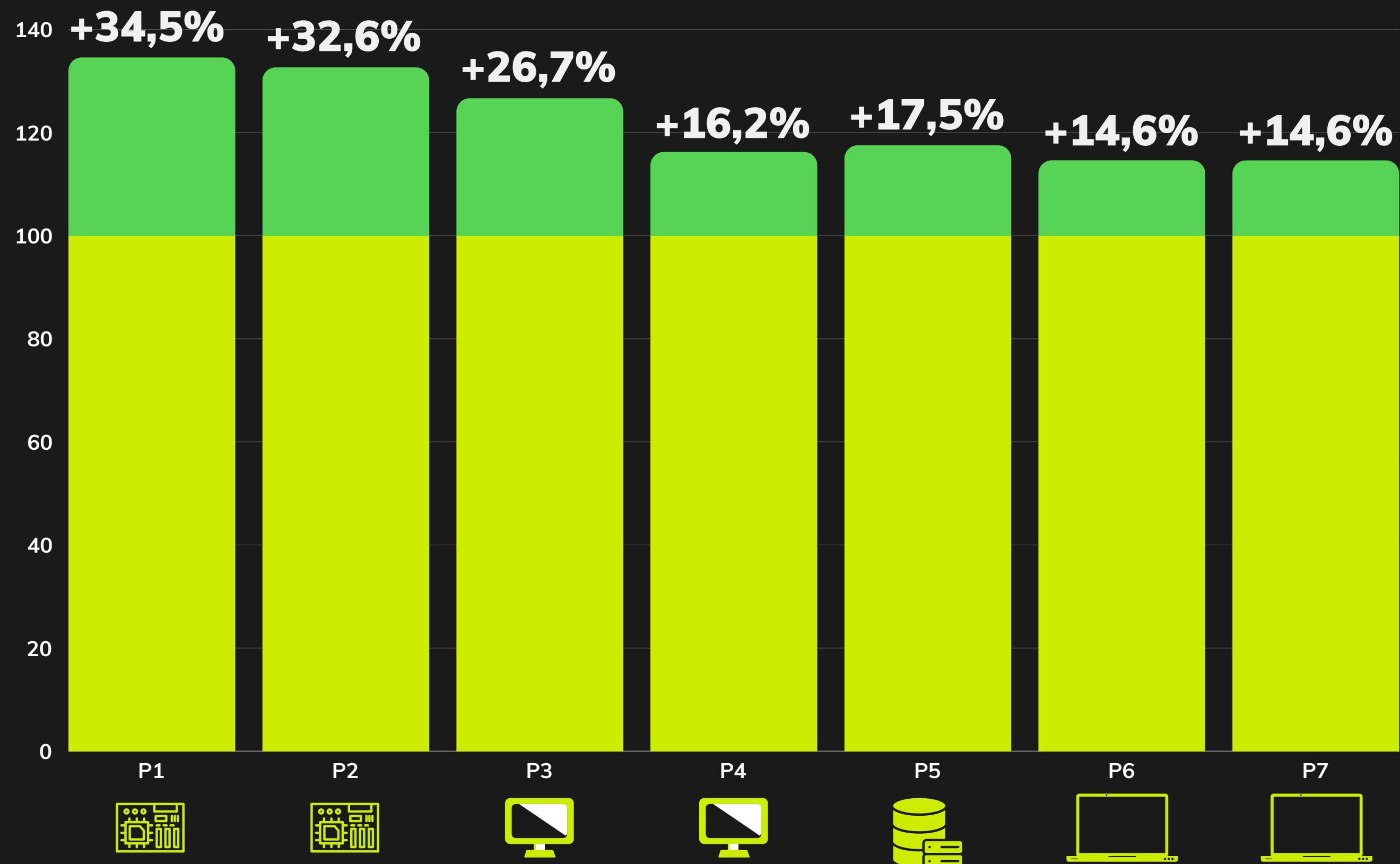


Ordenadores
ARM

ENTORNOS DE PRUEBAS

Nº	Familia	Modelo	Núcleos	Freq. (GHz)
1	ARM	RK3588S	4 + 4	2.4
2	ARM	RK3399	2 + 4	1.8
3	x86	Ryzen 7 1700	8	3
4	x86	i7 1185g7	4	3
5	x86	i9 13900K	8 + 16	3
6	ARM	M1 Pro	8	3.22
7	ARM	M1 Pro	8	3.22

COMPARATIVA

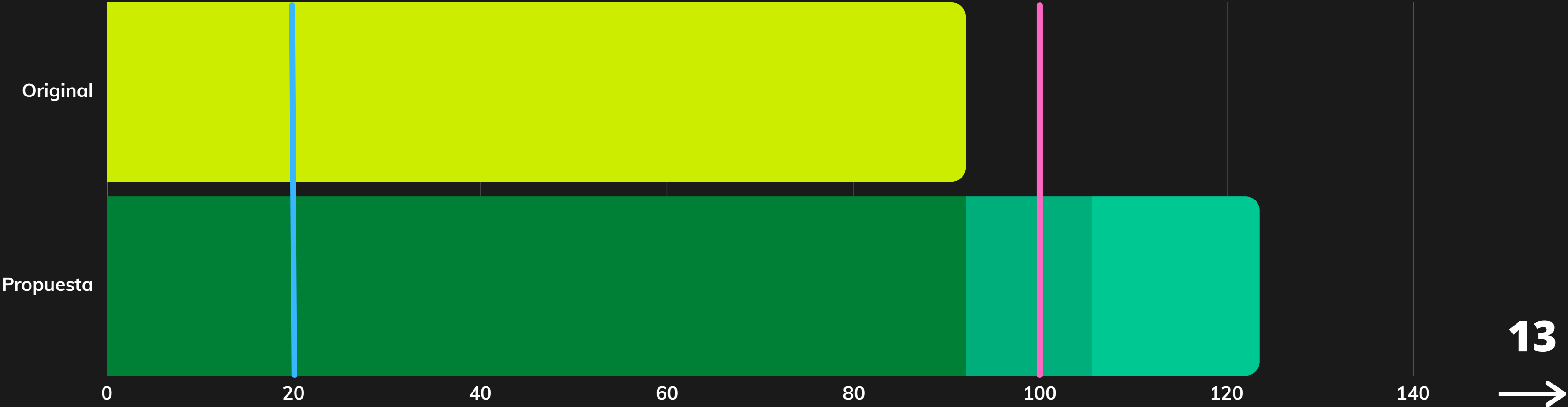


12



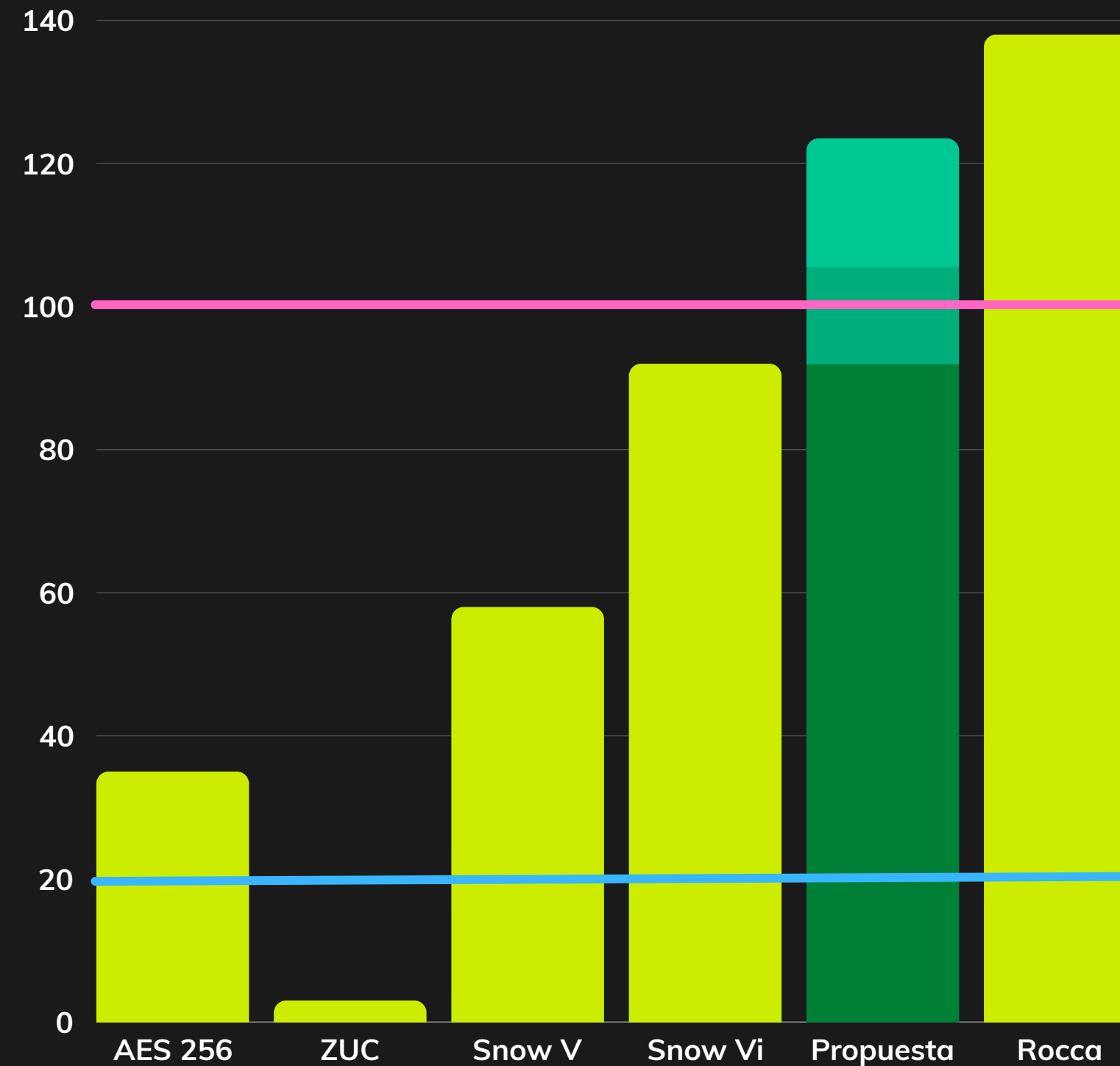
Resultados

+14,6% ~ +34,6%



VELOCIDADES

Comparativa de
velocidades
incluyendo la
propuesta



14



Conclusiones



**Muchas
gracias por
su atención**

email: gabiluisfreitas@gmail.com

email: alu0101348421@ull.edu.es