

The background is a dark blue-grey color. It is decorated with various geometric shapes in orange and white. In the top left, there is a large orange circle with a white dotted pattern inside. To its right is a white circle and an orange hexagon. Further right is a solid orange circle and a large orange trapezoid. In the top right, there are white dotted lines and a white triangle. On the left side, there is a white dotted hexagon, a solid orange circle, and a white circle with a small orange dot on its circumference. On the right side, there is a white dotted rectangle, a white triangle, and a large orange diamond with a white dotted pattern inside. At the bottom, there are orange hexagons, white dotted patterns, and overlapping orange and white circles.

Números Aleatorios y la Aleatoriedad Real

Grupo 12 – Batman

BERMÚDEZ, CALDERÓN, GONZALEZ PAUTASO

¿Para que se usan los números aleatorios?



Criptografía

Claves, números de sesión únicos y encriptación.



Simulaciones

Representar incertidumbre y variabilidad.



Entretenimiento

Videojuegos, Casino, Realidad Virtual

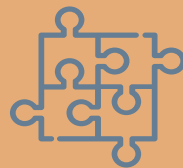
¿Cómo se generan los números aleatorios?

Pseudoaleatorios

Utilizan algoritmos matemáticos basados en una semilla inicial. Siguen un patrón si se conoce la semilla.

Aleatoriedad Real

Se basan en fenómenos físicos, como ruido térmico en circuitos electrónicos o fluctuación de voltaje. Requieren hardware especializado.



Implementaciones en arquitecturas

RDRAND

Instrucción Intel para números pseudoaleatorios

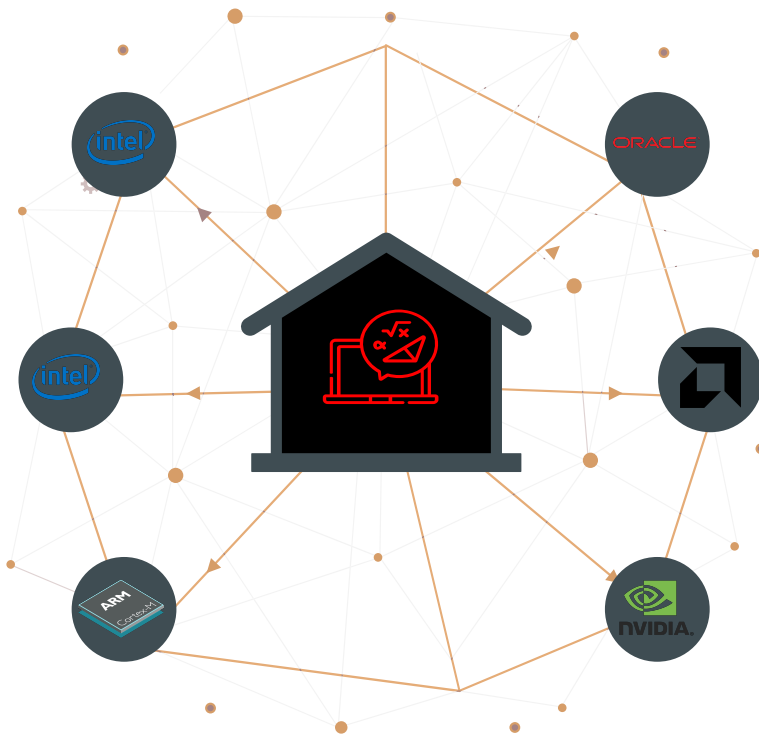
En hardware desde Ivy Bridge (2012)

RDSEED

Instrucción Intel para números realmente aleatorios

ARM TrustZone

Módulo de seguridad en procesadores ARM con TRNG (Celulares)



Oracle SPARC

Contiene módulos TRNG para bases de datos seguras.

AMD PSP

Microcontrolador en los procesadores AMD para gestionar la seguridad.

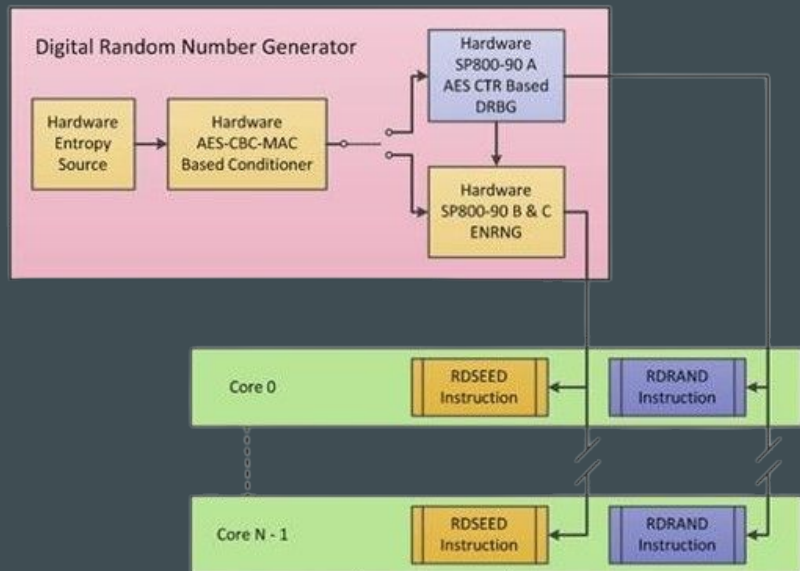
NVIDIA cuRAND

Usa los Cuda Cores para generar números pseudoaleatorios simultáneamente.



Ejemplo breve de un TRNG y PRNG

Módulo DRNG de Intel



Fuente de entropía

01.

Usa el ruido térmico dentro del silicio para producir bits aleatorios

Condicionador

02.

Se estabiliza la entropía en muestras de 256 bits

Alimentar los generadores

03.

DRBG para pseudoaleatorios. ENRNG para verdaderamente aleatorios.

Salidas vía instrucciones

04.

Los números generados se acceden mediante sus respectivas instrucciones

Objetivos

¿Qué esperamos aprender?

**Investigar
implementaciones**

**Impacto de los
TRNG y PRNG**

**Desafíos para
TRNGs fiables**





Gracias!

Dudas?

Fuentes:

[DRNG](#)

[Fotos PNG](#)

[Oracle SPARC](#)

[Nvidia cuRAND](#)

[ARM TrustZone](#)

[AMD psp](#)

CREDITS: This presentation template was created by **Slidesgo**, including icons by **Flaticon**, and infographics & images by **Freepik**.