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

En hardware desde Ivy Bridge (2012)

RDRAND

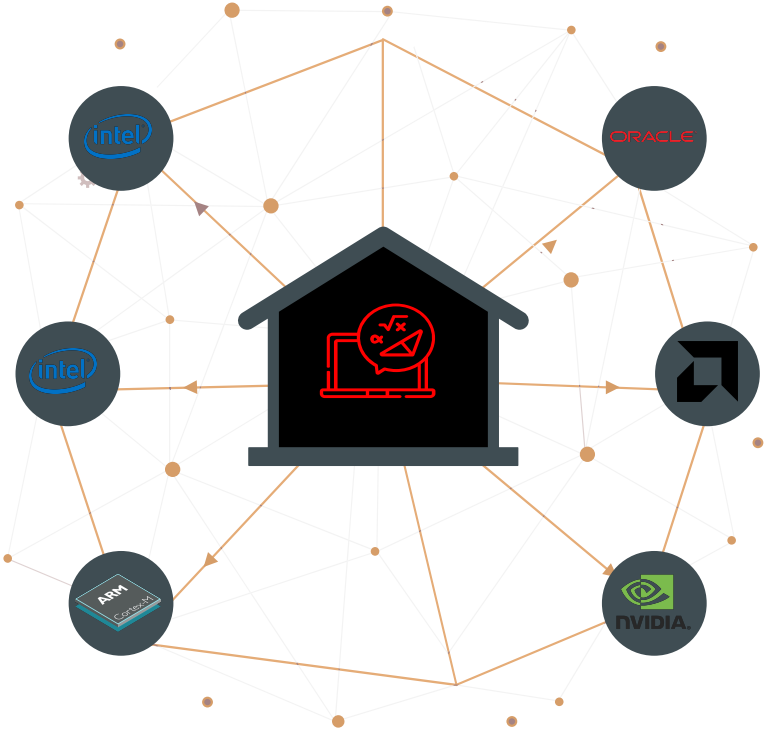
Instrucción Intel para números pseudoaleatorios

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.

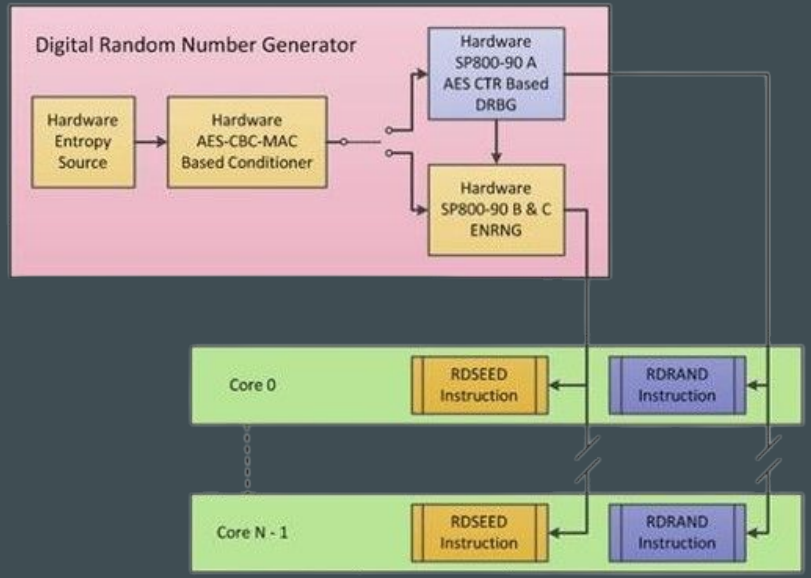
AMD PSP

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



01. **Fuente de entropía**

Usa el ruido térmico dentro del silicio para producir bits aleatorios

02. **Condicionador**

Se estabiliza la entropía en muestras de 256 bits

03. **Alimentar los generadores**

DRBG para pseudoaleatorios. ENRNG para verdaderamente aleatorios.

04. **Salidas vía instrucciones**

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.**