Dispositivo para la generación simultánea de identificadores y números verdaderamente aleatorios a partir de memorias de semiconductores (SRAMs)

El CSIC, en colaboración con la Universidad de Sevilla, ha desarrollado un dispositivo microelectrónico que permite generar simultáneamente identificadores de alta calidad y números verdaderamente aleatorios a partir de los valores iniciales de las memorias de semiconductores que utilizan celdas biestables (como las SRAMs). Los identificadores generados son únicos de esa memoria. Estudios experimentales demuestran que el método permite reducir la longitud de los identificadores, manteniendo la capacidad de identificación, en un 45% y que los bits requeridos para obtener plena entropía pueden reducirse en un 78%. El método se puede aplicar a diseños digitales estándares y puede ser realizado por el usuario final, sin necesidad de complejas configuraciones de laboratorio.

Se buscan socios industriales para la licencia de la patente

Resumen de la tecnología

Las celdas de memoria estáticas se caracterizan porque poseen dos estados estables manteniendo el dato binario que se les escribe, "0" ó "1", mientras están alimentadas y pierden la información si se les interrumpe la alimentación. Si se alimentan pero no se les escribe ningún dato, las celdas evolucionan hacia un valor u otro que es difícil de predecir. Es por ello casi imposible que un conjunto de celdas de memoria alcance los mismos valores de puesta en marcha.

El valor que alcanzan las celdas al ponerse en marcha es casi siempre el mismo. Esta singularidad permite su uso para generar identificadores. Sin embargo algunos bits tienden a modificar su valor con el tiempo, por cambios de temperatura o variaciones de la tensión de alimentación. Por ello, tiene que ser incorporado un mecanismo adicional de corrección de errores en los casos en los que los mismos valores de puesta en marcha quieran ser recuperados. Esto es lo que ocurre por ejemplo en la generación de claves criptográficas.

El método presentado minimiza la posible variación de los bits, por lo que reduce la complejidad de los algoritmos de corrección de errores o, de manera equivalente, reduce la longitud de los identificadores para obtener la misma capacidad de identificación.

Por otro lado, las celdas de memoria estática también se pueden utilizar para la generación de números verdaderamente aleatorios. En este caso, se aprovecha que las celdas de memoria no alcanzan los mismos valores de puesta en marcha en medidas sucesivas, por lo que son una fuente natural de entropía. El método desarrollado también permite aumentar la entropía de manera que se necesita acondicionar menos celdas para generar una semilla aleatoria de entropía total.

El método presentado permite generar identificadores y números verdaderamente aleatorios de forma simultánea, aumentando la velocidad y reduciendo el consumo de potencia necesario para generarlos y para extraer claves criptográficas.

Principales aplicaciones y ventajas

- El método evita la falsificación de productos digitales, porque los identificadores no se pueden clonar y son generados en el arranque de la memoria.
- El identificador (o clave criptográfica) no se almacena. De esta manera, se impide toda lectura no autorizada. La información almacenada no es sensible y puede ser revocada, por lo que no se requieren memorias no volátiles seguras.
- El método permite que las aplicaciones software se pueden vincular a un dispositivo físico con el fin de evitar que ningún otro dispositivo pueda ejecutar la aplicación.
- El método es un algoritmo simple que puede ser implementado como un hardware dedicado e incluido en el diseño digital.

Estado de la patente

Solicitud de patente española con posibilidad de extensión internacional

Para más información

Dr. José Ramón Domínguez Solís,
Vicepresidencia Adjunta de Transferencia de Conocimiento
Consejo Superior de Investigaciones Científicas (CSIC)
Tel.: + 34 – 95 423 23 49
E-mail: jrdominguez@orgc.csic.es