Case ID:M16-020P^

Published: 2/26/2020

Inventors

Lawrence Clark

Keith Holbert

James Adams

Contact

Shen Yan
shen.yan@skysonginnovations.com

Secure true random number generation using 1.5-T transistor flash memory

Flash memory and true random number generators (TRNGs) can be essential components of security systems for smart devices. Using physical variations in integrated circuit (IC) constituent components is an increasingly popular technique for generating true random numbers. An existing approach uses a technique called "partial programming" to take an element to a point of instability, where its state can flip to either "0" or "1". Sequential elements in an array do the same thing, thereby creating a random number based on the state flips. However, the programming speed is too fast and can be difficult to tune to the mid-way instability point. Furthermore, systematic errors may occur across an array due to fabrication that tends to make flips less than truly random. Therefore, there is a need for a controllable and truly random number generator.

Researchers at Arizona State University have created a true random number generator based on a 1.5-T transistor flash memory. This approach uses a method called "partial erasing". Partial erasing is a slower and more controllable process that allows the mid-point for instability to be reached with more certainty. Additionally, interleaving and combining different areas of an array can be used to overcome systematic variation and makes the process truly random.

Potential Applications

- Microelectronics
- Microchips and integrated circuits
- Security systems
- Smart Devices

Benefits and Advantages

- More controlled process - Uses "partial erasing", which is a slower and more controllable process, allowing the mid-point for instability to be reached with much more certainty.
- Truly random –
  - The quality has been quantified by passing the NIST randomness tests.
  - Systematic correlations can be removed while retaining the essential randomness and thus providing high quality TRNG functionality.

For more information about the inventor(s) and their research, please see

Dr. Lawrence Clark's directory webpage

Dr. Keith Holbert's directory webpage