In the Name of God

A Summary of

Digital Randomness

by Sadegh Hayeri
(Student ID#810194298, Group: Wednesday 10:00 to 12:00 AM)

The article describes Intel's digital random number generation architecture. Generating completely random numbers is essential for secure applications like online banking or password encryption. Early random number generators used inherently random analog signals like thermal noise to produce random numbers. Unfortunately, analog circuits consume much more energy than digital ones and are harder to maintain and improve. As a result, they are not suitable for today's computation and energy demands. The digital random number generator introduced in this article consists of two inverter gates. The input of each gate is connected to the output of the other one. In the stable state of this system, one inverter outputs 0 and the other one outputs 1. If a temporary signal forces both of these outputs to be 1, the inverters enter an unstable state. As soon as the signal is turned off, the system must choose one of the two possible stable states. The choice is based on conditions like temperature or subtle differences in the gates. Hence, this choice produces a relatively random bit. This bit is not perfectly random because differences in the inverters might always bias the output one way or the other. Intel applies a series of numerical procedures (not described in the article) to ensure perfect randomness. A drawback of these procedures is that it makes the generation process slow. Hence, as a final touch, Intel uses these randomly generated numbers to initiate the seed of a fast algorithmic pseudo-random generator The article reports that this new architecture is faster and more suitable to random number generation demands than its predecessors.

Ref. G. Taylor and G. Cox, “Digital randomness,” IEEE SPECTRUM, pp. 32-35, 56-58, Sep. 2011